

Joint Publication 3-51



Joint Doctrine for Electronic Warfare



7 April 2000



Report Documentation Page		
Report Date 07042000	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Joint Doctrine for Electronic Warfare	Contract Number	
	Grant Number	
	Program Element Number	
Author(s)	Project Number	
	Task Number	
	Work Unit Number	
Performing Organization Name(s) and Address(es) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102	Performing Organization Report Number	
Sponsoring/Monitoring Agency Name(s) and Address(es) Joint Chiefs of Staff	Sponsor/Monitor's Acronym(s)	
	Sponsor/Monitor's Report Number(s)	
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes The original document contains color images.		
Abstract		
Subject Terms IATAC COLLECTION		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 108		

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> OMB No. 074-0188	
<small>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503</small>				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 4/7/2000	3. REPORT TYPE AND DATES COVERED Publication 4/7/2000	
4. TITLE AND SUBTITLE Joint Doctrine for Electronic Warfare			5. FUNDING NUMBERS	
6. AUTHOR(S) Joint Chiefs of Staff				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Joint Chiefs of Staff			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This publication establishes doctrinal guidance on the use of electronic warfare (EW) in joint operations. Specifically, the following areas are within the scope of this publication: the fundamentals of EW; the staff organization and command relationships of EW in joint operations; planning procedures for joint EW; coordination of joint EW during operations; training and exercise considerations for EW in joint operations; and allied and coalition considerations in planning and conducting joint EW.				
14. SUBJECT TERMS IATAC Collection, Joint, Doctrine, electronic warfare,			15. NUMBER OF PAGES	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	

PREFACE

1. Scope

This publication establishes doctrinal guidance on the use of electronic warfare (EW) in joint operations. Specifically, the following areas are within the scope of this publication: the fundamentals of EW; the staff organization and command relationships of EW in joint operations; planning procedures for joint EW; coordination of joint EW during operations; training and exercise considerations for EW in joint operations; and allied and coalition considerations in planning and conducting joint EW.

2. Purpose

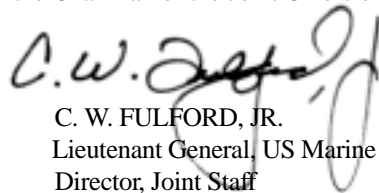
This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander (JFC) from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

For the Chairman of the Joint Chiefs of Staff:



C. W. FULFORD, JR.
Lieutenant General, US Marine Corps
Director, Joint Staff

Intentionally Blank

TABLE OF CONTENTS

	PAGE
EXECUTIVE SUMMARY	vii
CHAPTER I	
OVERVIEW OF ELECTRONIC WARFARE	
• Introduction	I-1
• Electromagnetic Environment	I-1
• Military Operations and the Electromagnetic Environment	I-1
• Role of Electronic Warfare in Military Operations	I-1
• EW as a Part of Other Military Concepts	I-4
• Directed Energy as a Part of EW	I-4
• Principal EW Activities	I-5
• Intelligence and Electronic Warfare Support	I-8
• Service Perspectives of EW	I-8
CHAPTER II	
ORGANIZING FOR JOINT ELECTRONIC WARFARE	
• Introduction	II-1
• Joint EW Organization	II-1
• Joint EW Staff Manning	II-2
• Joint Frequency Management Organization	II-3
• Organization of Intelligence Support to EW	II-4
• Service Organization for EW	II-5
CHAPTER III	
PLANNING JOINT ELECTRONIC WARFARE	
• Introduction	III-1
• EW Planning Considerations	III-1
• Joint EW Planning Process	III-6
• EW Planning Guidance	III-9
• EW Planning Aids	III-10
CHAPTER IV	
COORDINATING JOINT ELECTRONIC WARFARE	
• Introduction	IV-1
• Joint Coordination and Control	IV-1
• EW Frequency Deconfliction	IV-7
• Component Coordination Procedures	IV-10
• EW and Intelligence Coordination	IV-12

CHAPTER V

ELECTRONIC WARFARE IN JOINT EXERCISES

• Introduction	V-1
• Planning Joint Exercises	V-1
• Planning EW in Joint Exercises	V-1
• EW in Exercise Preparation, Execution, and Post-Exercise Evaluation	V-7

CHAPTER VI

MULTINATIONAL ASPECTS OF ELECTRONIC WARFARE

• Introduction	VI-1
• MNF EW Organization and Command and Control	VI-1
• Multinational EWCC with NATO Forces	VI-3
• Multinational EW with ABCA and ASCC Member Nations	VI-3
• Multinational EWCC with Non-NATO or ABCA Allies or Coalition Partners	VI-3
• EW Mutual Support	VI-3
• Releasability of EW Information to Allies and Multinational Forces	VI-5

APPENDIX

A JOPES Electronic Warfare Guidance	A-1
B Electronic Warfare Frequency Deconfliction Procedures	B-1
C Joint Spectrum Center Support to Joint Electronic Warfare	C-1
D Electronic Warfare Reprogramming	D-1
E Electronic Warfare Modeling	E-1
F Service Perspectives of Electronic Warfare	F-1
G References	G-1
H Administrative Instructions	H-1

GLOSSARY

Part I Abbreviations and Acronyms	GL-1
Part II Terms and Definitions	GL-4

FIGURE

I-1 Portions of the Electromagnetic Spectrum	I-2
I-2 Concept of Electronic Warfare	I-3
I-3 Information Operations: Capabilities and Related Activities	I-5
II-1 Duties Assigned to the Electronic Warfare Officer	II-2
II-2 Organization of Intelligence Support to Electronic Warfare	II-4
III-1 Joint Frequency Management Office Spectrum Management Process	III-2
III-2 Joint Task Force Electromagnetic Spectrum Management Planning Flow	III-3
III-3 Electronic Warfare Planning Related to Deliberate Planning	III-7
III-4 Electronic Warfare Planning Related to Crisis Action Planning	III-8
IV-1 Executing Wartime Frequency Use	IV-2

IV-2 Electronic Warfare Activities Coordinated With Information Operations
Activities IV-4

IV-3 Critical Elements in the Electronic Warfare Frequency Deconfliction
Process IV-8

V-1 Electronic Warfare Exercise Planning Flow V-2

V-2 Tasks to Integrate Electronic Warfare Into Joint Exercises V-4

V-3 Stages of a Joint Exercise V-7

Intentionally Blank

EXECUTIVE SUMMARY

COMMANDER'S OVERVIEW

- Provides an Overview of Electronic Warfare
 - Covers Organizing for Joint Electronic Warfare
 - Discusses Planning and Coordination Requirements for Joint Electronic Warfare
 - Identifies Electronic Warfare Requirements in Joint Exercises
 - Covers Multinational Aspects of Electronic Warfare
-

Introduction

The three major subdivisions of electronic warfare (EW) are electronic attack, electronic protection, and electronic warfare support.

Military operations are executed in an **increasingly complex electromagnetic environment**. Electromagnetic (EM) energy occurs naturally or can be manmade. This energy, in the form of EM radiation, is made up of oscillating electric and magnetic fields and is propagated at or near the speed of light. **The EM environment** is a combination of the power, frequency, and duration of the radiated or conducted EM emissions that may be encountered by a military force. The term “electromagnetic spectrum” refers to the range of frequencies of EM radiation from zero to infinity. In military operations, the term **electronic warfare (EW)** refers to any military action involving the use of electromagnetic or directed energy to control the EM spectrum or to attack the enemy. EW includes three major subdivisions: **electronic attack, electronic protection, and electronic warfare support (ES)**. The need for control of the EM spectrum and the type of EW actions that can be used to control that spectrum depend on the operational environment in which a military operation is carried out. In joint operations, EW is a military capability that must be integrated into a given joint operation as it supports all phases and aspects of a campaign. The principal activities used in EW have been developed over time to **exploit the opportunities and vulnerabilities which are inherent in the physics of EM energy**. The distinction between intelligence and ES is determined by who tasks or controls the intelligence assets, what they are tasked to provide, and for what purpose they are tasked. ES is achieved by intelligence collection, processing, and exploitation assets tasked or controlled by an operational commander for immediate threat

recognition and other tactical actions such as threat avoidance, targeting, and homing.

Organizing for Electronic Warfare

The joint force commander, Plans Directorate, and Operations Directorate will have primary responsibility for the planning, coordination, and integration of joint force EW operations.

How joint forces are organized to plan and execute EW is a prerogative of the **joint force commander (JFC)**. EW has operational implications for planning and supervision functions that are normally divided among several directorates of a joint staff. Authority for long range planning is normally **delegated by the JFC to the Plans Directorate** and supervising joint EW **delegated to the Operations Directorate (J-3)**. As one of the capabilities of information operations (IO), EW is planned in close coordination with other staff functions. Normally, the **EW officer is the principal staff EW planner** on a joint staff. The scope and nature of the EW officer's responsibilities is dependent on the size of the staff, the operational area of the JFC which the staff supports, and the type of mission or operation which the staff must plan. The requirement for staff personnel to support the EW officer varies among joint staffs. Accomplishment of this work requires that the core members of a staff assisting the EW officer have a **depth of technical expertise and knowledge** of the capabilities of EW systems currently employed by components, allies, and coalition partners. Augmentation of joint staffs during times of crisis or impending operations in order to accumulate additional EW expertise is almost always necessary. It is important to note that each Military Service has a different approach to organizing their forces to plan and execute EW.

Planning

Since EW must not conflict with military operations and others using the electromagnetic (EM) spectrum, it is essential that EW planners coordinate their planned activities with them.

EW is a complex aspect of modern military operations that must be **fully integrated with other aspects of joint operations** in order to achieve its full potential for contributing to an operation's objectives. Such integration **requires careful planning**. EW is only one type of activity that occurs in an increasingly crowded EM spectrum. As such, EW planners must be concerned with coordinating their planned activities with other aspects of military operations that use the EM spectrum as well as third party users of the spectrum that EW does not wish to disrupt. Like other aspects of joint operations, joint EW is **centrally planned and decentrally executed**. Since the Military Services provide most US EW assets available in joint operations, Service component EW planners should be integrated into the joint planning process. Since EW activity takes place in the EM spectrum, joint EW planners must closely coordinate their efforts with those members of the joint staff

who are concerned with managing military use of the EM spectrum. Military operations dependence on EM energy and use of the EM spectrum by the systems that sense, process, store, measure, analyze, and communicate information create **IO opportunities and vulnerabilities** that EW can address. The purpose of **EW reprogramming** is to maintain or enhance the effectiveness of EW and target sensing system equipment employed by tri-Service units. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems. Effective electronic masking of joint military operations involves the proactive management of all friendly radiated electronic signatures of equipment being used in or supporting the operation. **Interoperability is essential** to use EW effectively as an element of joint military power. The major requirements of interoperability are to establish standards and practice procedures that allow for integrated planning and execution of EW operations (including joint EW) as well as timely and routine exchange of EW information. Like other aspects of joint operations, joint **EW planning is conducted through the Joint Operation Planning and Execution System (JOPES) process**. In order to be fully integrated into other aspects of a planned operation, EW planning must start in the earliest stages of the JOPES process and be coordinated with other aspects of the plan every step of the way. Planning guidance for EW should be included in an operation plan (OPLAN) as a tab to the IO guidance. There are a number of automated planning tools available to help joint EW planners carry out their responsibilities.

Coordinating

EW staff should focus on coordination efforts that ensure EW actions are carried out as planned, with emphasis on EW asset allocation, EM spectrum management, and emerging operational issues.

Once a plan has been approved and an operation is commenced, the preponderance of EW staff effort shifts to the **coordination necessary to ensure that EW actions are carried out as planned or modified** to respond to the dynamics of the operation. EW staff personnel have a major role to perform in the dynamic management of the EM spectrum during operations. Most of the elements and activities of **IO depend on, use, or exploit the EM spectrum** for at least some of their functions. The deconfliction and coordination of EW activities in an operation is a continuous process for the IO cell and EW staff personnel. Exploitation of adversary equipment can verify adversary electronic equipment capabilities, to include wartime reserve modes. There are several **critical elements in the EW frequency deconfliction process** that should be performed on a continuing basis. Components requiring EW support from another component should be

encouraged to **directly coordinate** that support when possible, informing joint EW planners of the results of such coordination. **Detailed coordination** is essential between the EW activities and the intelligence activities supporting an operation.

Joint Exercises

EW exercise activities must be well-planned to balance EW training objectives with other training objectives.

Joint exercises are a unique opportunity to exercise component EW capabilities in mutually supportive operations. Exercise planning is a separate process from the JOPEs planning that is used to develop OPLANs. The command or person designated to plan the EW aspects of an exercise must be concerned with: (1) **identifying EW exercise objectives that are consistent with the overall exercise objectives in scope, purpose, and level of effort**; (2) developing an **EW concept of operations that is integrated into the larger IO concept of operations**; (3) **coordinating EW personnel and assets** to participate as both “Blue” and “Red” forces; (4) **identifying personnel with EW expertise** to participate as joint exercise control group and “white cell” participants; (5) **determining EW modeling and simulation requirements and systems** for the exercise and coordinating their availability and funding; and (6) **drafting the EW sections of the exercise directive and supporting plans** such as the exercise control plan. The planning stage is only the first of four stages in the life cycle of each joint exercise. The other three stages, **preparation, execution, and post-exercise and evaluation**, also involve tasks and coordination on the part of EW exercise staff personnel.

Multinational Aspects of EW

US planners must provide EW support to allied or coalition nations, as EW is an integral part of multinational operations.

US planners must be prepared to **integrate US and allied or coalition EW capabilities** into an overall EW plan; be able to provide allied or coalition nations with information concerning US EW capabilities within releasability guidelines; and provide EW support to allied or coalition nations. In US-led operations, the doctrine within this publication should be used as the basis for all EW activities within the Multinational Force (MNF). However, the planning of MNF EW is made more difficult because of **ill-defined security issues, different crypto equipment, differences in the level of training of involved forces, and language barriers**. The MNF commander (MNFC) provides guidance for planning and conducting EW operations to the MNF through the **J-3 and the IO cell**. The MNFC should assign responsibilities for management of EW resources in multinational operations among the staff. North Atlantic Treaty Organization's (NATO's) EW doctrine, contained in Military Committee Document 64/8, “NATO

Electronic Warfare Policy,” is largely **based on US EW doctrine**.

CONCLUSION

The focus of this publication is to provide guidance on the use of EW in joint operations. The material is focused specifically on the fundamentals of EW; the staff organization and command relationships of EW in joint operations; planning procedures for joint EW; coordination of joint EW during operations; training and exercise considerations for EW in joint operations; and allied and coalition considerations in planning and conducting joint and/or combined EW.

Intentionally Blank

CHAPTER I

OVERVIEW OF ELECTRONIC WARFARE

"There is much more to electronic warfare than simply detecting enemy transmissions."

Martin Van Creveld
Technology and War, 1989

1. Introduction

Military operations are executed in an increasingly complex electromagnetic environment (EME). Today, electromagnetic (EM) devices are used by both civilian and military organizations for **communications, navigation, sensing, information storage, and processing**, as well as a variety of other purposes. The increasing portability and affordability of sophisticated EM equipment guarantees that the EME in which military forces operate will become **more complex in the future**. The recognized need for military forces to have unimpeded access to and use of the EME creates **vulnerabilities and opportunities for electronic warfare (EW)** in support of military operations. In joint operations, EW is one of the integrated capabilities **used to conduct information operations (IO)**.

2. Electromagnetic Environment

EM energy occurs **naturally or can be manmade**. This energy, in the form of EM radiation, is made up of oscillating electric and magnetic fields and is propagated at or near the speed of light. **EM radiation** is measured by the frequency of its wave pattern's repetition within a set unit of time. The standard term for the measurement of EM radiation is the hertz, the number of repetitions (cycles) per second. The term **"electromagnetic spectrum"** refers to the range of frequencies of EM radiation from zero to infinity. The spectrum is divided into alphabetically designated bands which range

from radio frequencies at the low end to infrared and optical frequencies at the high end of the spectrum. Figure I-1 depicts that portion of the EM spectrum used principally in military applications. The operational **EME** is a combination **of the power, frequency, and duration of the** EM emissions that may be encountered by a military force while performing its assigned mission.

3. Military Operations and the Electromagnetic Environment

The impact of the EME upon the operational capability of military forces, equipment, systems, and platforms is referred to as **electromagnetic environmental effects (E3)**. E3 encompasses **all EM disciplines**, including EM compatibility and interference; electronic protection (EP), hazards of EM radiation to ordnance (HERO), and volatile materials such as fuels; and the natural phenomena effects of lightning and precipitation static. Equipment and systems that operate on the principles of electromagnetism are characterized by **EM vulnerability** that causes them to **suffer a definite degradation** (incapability to perform the designated mission) as a result of having been subjected to a certain level of E3.

4. Role of Electronic Warfare in Military Operations

a. In military operations, the term EW refers to any military action involving the **use of EM or directed energy to control the EM**

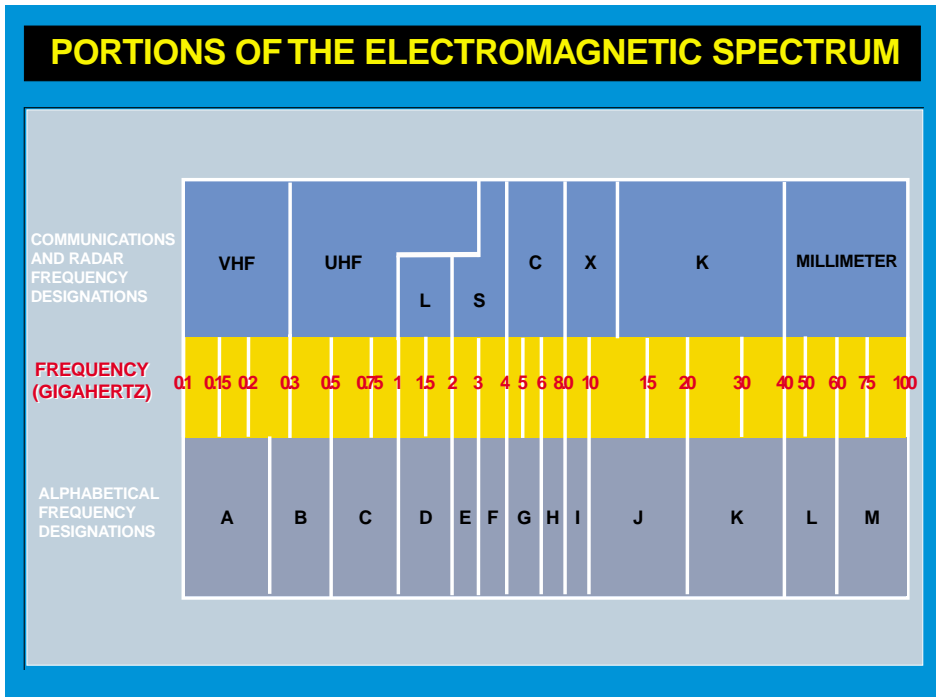


Figure I-1. Portions of the Electromagnetic Spectrum

spectrum or to attack the enemy. EW includes three major subdivisions: electronic attack (EA), EP, and electronic warfare support (ES). Figure I-2 gives a conceptual view of EW, the relationships of the three subdivisions, and the relationship of the subdivisions to principal EW activities.

- **Electronic Attack.** EA is the subdivision of EW involving the use of **EM energy, directed energy, or antiradiation weapons** to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (see Joint Publication [JP] 3-09, “Doctrine for Joint Fire Support”). EA includes:

- actions taken to prevent or reduce an enemy’s effective use of the EM spectrum, such as jamming and EM deception; and

- employment of weapons that use either EM or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, or particle beams).

- **Electronic Protection.** EP is the subdivision of EW involving passive and active means taken to **protect personnel, facilities, and equipment** from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability.
- **Electronic Warfare Support.** ES is the subdivision of EW involving actions tasked by, or under direct control of, an operational commander **to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy** for the purpose of immediate threat recognition, targeting, planning, and

CONCEPT OF ELECTRONIC WARFARE

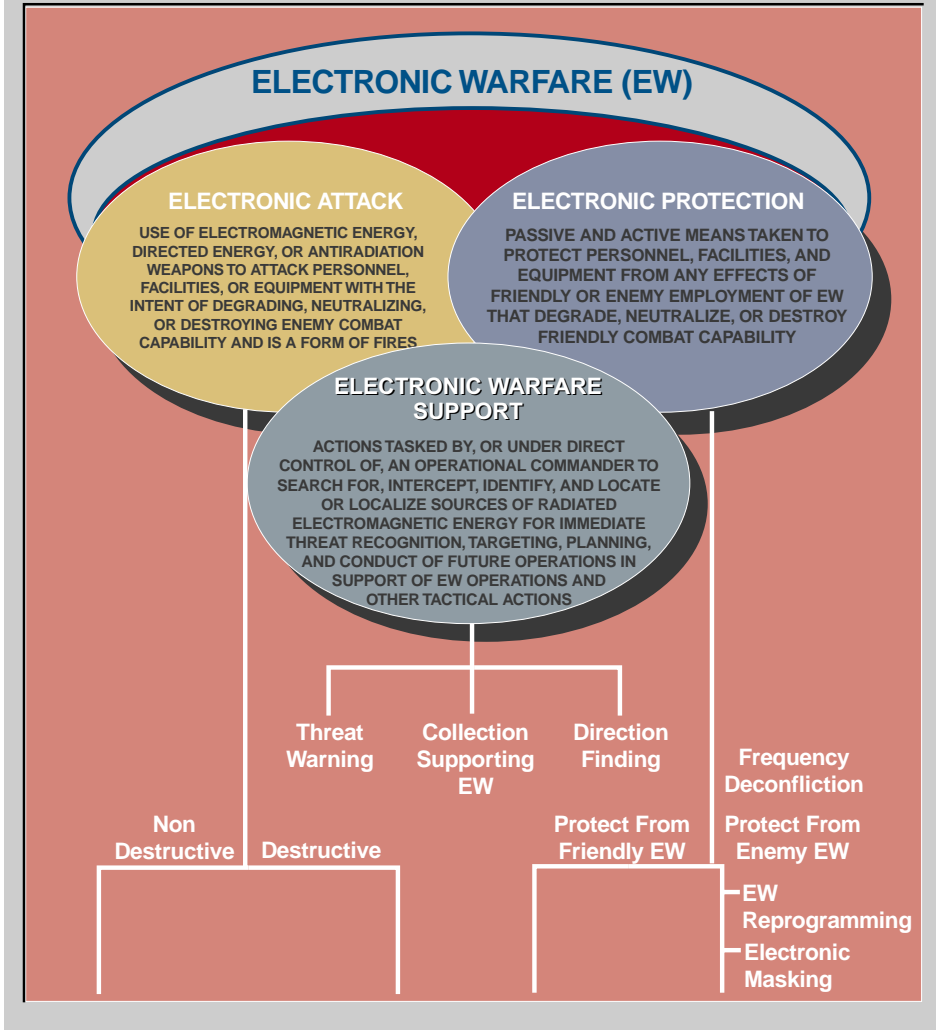


Figure I-2. Concept of Electronic Warfare

conduct of future operations. ES provides information required for decisions involving EW operations and other tactical actions such as threat avoidance, targeting, and homing. ES data can be used to produce signals intelligence (SIGINT), provide targeting for electronic or destructive attack, and produce measurement and signature intelligence (MASINT). SIGINT can

also provide battle damage assessment and feedback on the effect of the overall operational plan.

b. EW is waged throughout the EM spectrum in order **to secure and maintain effective control and use of the spectrum** by friendly forces and to deny use by an adversary through damage, destruction, disruption, and deception. The need for

control of the EM spectrum and the type of EW actions that can be used to control that spectrum depend on the operational environment in which a military operation is carried out.

- In peacetime, **intergovernmental bodies, governmental bodies, and law** control use of the EM spectrum. However, standing rules of engagement emphasize the joint force commanders' (JFCs') responsibility at all times to take appropriate and necessary action to protect their forces. EW measures that are normally not permitted in peacetime should be included in such action.
- In military operations that involve the use or threat of force, **control of the EM spectrum will often be contested** and the full range of EW actions may be considered. The type and level of EW actions appropriate to a particular military operation depend on the threat which adversary forces pose, the reliance of adversary forces on use of the EM spectrum, and the objectives of the operation.

5. EW as a Part of Other Military Concepts

In joint operations, EW is one of the military capabilities that are **integrated to conduct IO**. IO seek to affect adversary information and information systems while defending friendly information and information systems. IO strategies support military missions and are in consonance with guidance provided in the United States' Unified Command Plan, Joint Strategic Capabilities Plan, and Defense Planning Guidance documents. These strategies require integrated and synchronized offensive, defensive, and exploitive actions to counter, protect against, and learn of threats presented at any given time. These actions can be categorized by several supporting

activities such as operations security (OPSEC), military deception, psychological operations (PSYOP), EW, physical destruction or physical protection, computer network attack (CNA), and computer network defense (CND). Since the collection, processing, storage, and transmission of information often rely on EM energy, **EW is an essential part of IO** (see Figure I-3). **Information warfare** is IO conducted during time of crisis or conflict. EW also has an important role to play in **the suppression of enemy air defenses (SEAD)**. EW's role in these concepts is discussed further in Chapter III, "Planning Joint Electronic Warfare."

For more information on joint IO doctrine, refer to JP 3-13, "Joint Doctrine for Information Operations." For more information on joint tactics, techniques, and procedures for conducting SEAD, refer to JP 3-01.4, "Joint Tactics, Techniques, and Procedures for Joint Suppression of Enemy Air Defenses (J-SEAD)."

6. Directed Energy as a Part of EW

Directed energy (DE) is an umbrella term covering technologies that relate to the production of a beam of concentrated EM energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to **damage or destroy adversary equipment, facilities, and personnel**. **Directed-energy warfare (DEW)** is military action involving the use of DE weapons, devices, and countermeasures to either **cause direct damage or destruction** of adversary equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the EM spectrum through damage, destruction, and disruption. It also includes actions taken to **protect friendly equipment, facilities, and personnel and retain friendly use of the EM spectrum**. Possible applications include lasers, radio frequency weapons, and particle

INFORMATION OPERATIONS: CAPABILITIES AND RELATED ACTIVITIES

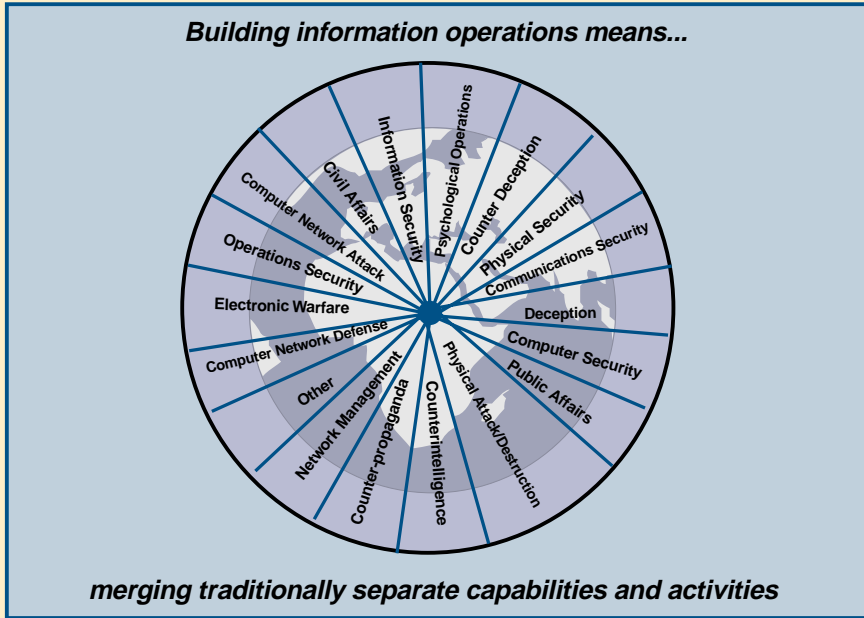


Figure I-3. Information Operations: Capabilities and Related Activities

beam weapons. As the development of DEW evolves, tactics, techniques, and procedures must also evolve to ensure their safe, effective employment. Although some DE applications will easily fit into traditional EW roles, others will not. For example, a laser designed to blind or disrupt optical sensors is, in EW terms, EA. A laser warning receiver designed to detect and analyze a laser signal is, in EW terms, ES. A visor or goggle designed to filter out the harmful wavelength of laser light is, in EW terms, EP. The threat of an adversary's use of destructive DE weapons and other destructive radio frequency weapons is also growing. Intelligence assets must be tasked to collect information about this threat, and joint planning must include the concerted development of operational procedures and courses of action (COAs) to mitigate the effects of adversaries' use of these weapons against friendly forces.

7. Principal EW Activities

The principal activities used in EW have been developed over time to **exploit the opportunities and vulnerabilities that are inherent in the physics of EM energy**. Although new equipment and new tactics continue to be developed, the physics of EM energy remains constant. This physical constant is the reason that the basic activities of EW remain effective despite changes in hardware and tactics.

The principal activities used in EW include the following.

a. **Electromagnetic Compatibility.** **Electromagnetic compatibility (EMC)** is the ability of systems, equipment, and devices that utilize the EM spectrum to operate in their intended operational environments

FIRST RECORDED INSTANCE OF DELIBERATE RADIO JAMMING

The first recorded instance of deliberate radio jamming took place in September 1901, in the [United States]. Interestingly, it was aimed at securing commercial gain rather than military advantage. As now, there was considerable public interest in the America's Cup yacht races, and the newspaper first to reach the stands carrying each result stood to reap a large profit . . . A third company . . . failed to get a sponsor but . . . used a transmitter more powerful than its competitors, and one of its engineers, John Pickard, worked out a method which allowed him to jam signals from the other companies while at the same time reporting on the progress of the race from his boat.

SOURCE: Alfred Price
The History of U.S. Electronic Warfare, Volume I, 1984

without suffering unacceptable degradation or causing unintentional degradation because of EM radiation or response. EMC involves the application of sound EM spectrum management: system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.

b. **Electromagnetic Deception.** EM deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner **intended to convey misleading information to an enemy** or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of EM deception are the following.

- **Manipulative EM Deception.** This type of deception involves actions to eliminate revealing, or convey misleading, EM telltale indicators that may be used by hostile forces.
- **Simulative EM Deception.** This type of deception involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.

- **Imitative EM Deception.** This type of deception introduces EM energy into enemy systems that imitates enemy emissions.

c. **Electromagnetic Hardening.** EM hardening consists of actions taken to protect personnel, facilities, and equipment by **filtering, attenuating, grounding, bonding, and shielding** against undesirable effects of EM energy.

d. **Electromagnetic Interference.** **EM interference (EMI)** is any EM disturbance that **interrupts, obstructs, or otherwise degrades or limits the effective performance** of electronics or electrical equipment. It can be induced intentionally, as in some forms of EW, or unintentionally, as a result of spurious emissions and responses, and intermodulation products.

e. **Electromagnetic Intrusion.** EM intrusion is the intentional insertion of EM energy into transmission paths in any manner, with the objective of **deceiving operators or causing confusion**.

f. **Electromagnetic Jamming.** EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the

purpose of **preventing or reducing an enemy's effective use of the EM spectrum**, with the intent of degrading or neutralizing the enemy's combat capability.

g. **Electromagnetic Pulse.** EM pulse is **a strong electronic pulse, most commonly caused by a nuclear explosion** that may couple with electrical or electronic systems to produce damaging current and voltage surges.

h. **Electronic Masking.** Electronic masking is the **controlled radiation of EM energy on friendly frequencies** so as to protect the emissions of friendly communications and electronic systems against enemy ES measures or SIGINT, without significantly degrading the operation of friendly systems.

i. **Electronic Probing.** Electronic probing is the **intentional radiation designed to be introduced into the devices or systems of potential enemies** for the purpose of learning the functions and operational capabilities of the devices or systems.

j. **Electronic Reconnaissance.** Electronic reconnaissance is **the detection, location, identification, and evaluation of EM radiations**.

k. **Electronic Intelligence.** **Electronic intelligence (ELINT)** is the technical and geolocational **intelligence derived from foreign non-communications EM radiations** emanating from other than nuclear detonations or radioactive sources.

l. **Electronics Security.** Electronics security is the protection resulting from all measures designed to **deny unauthorized persons information of value** that might be derived from their interception and study of noncommunications EM radiations, e.g., radar.

m. **Electronic Warfare Reprogramming.** EW reprogramming is the deliberate **alteration or modification of EW or target sensing systems (TSSs)** in response to validated changes in equipment, tactics, or the EME. These changes may be the result of deliberate actions on the part of friendly, adversary, or third parties or may be brought about by EMI or other inadvertent phenomena. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and TSS equipment. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems.

n. **Emission Control.** **Emission control (EMCON)** is the selective and controlled use of EM, acoustic, or other emitters to **optimize command and control (C2) capabilities** while minimizing, for operations security:

- detection by enemy sensors;
- mutual interference among friendly systems; and
- inhibitors to executing a military deception plan.

o. **Spectrum Management.** Spectrum management involves planning, coordinating, and managing use of the EM spectrum through **operational, engineering, and administrative procedures**. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

p. **Wartime Reserve Modes.** Wartime reserve modes (WARM) are characteristics and operating procedures of sensors, communications, navigation aids, threat recognition, weapons, and countermeasures systems **that will contribute to military effectiveness if unknown to or**

FIRST US ELECTRONIC INTELLIGENCE SATELLITE

Following the loss of the U-2, President Eisenhower ordered that no further overflights be made by these planes over the USSR. But as that door was closed to the intelligence collectors, another opened. Within a few weeks the first US ELINT [electronic intelligence] collection satellite was launched from the Cape Canaveral test site. The early ELINT satellites were fitted with a simple broad-band transponder covering the DE [directed energy] bands, which picked up radar signals and immediately rebroadcast them on a different frequency to be picked up by US ground stations around the world. It was the start of a program that would continue, with increasing complexity and capability, to the present day.

SOURCE: Alfred Price
The History of U.S. Electronic Warfare, Volume II

misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. WARM are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use.

8. Intelligence and Electronic Warfare Support

Electronic forms of intelligence gathering (SIGINT, MASINT, and other forms) comprise a significant portion of the day-to-day activities of the intelligence community. The distinction between intelligence and ES is determined by who tasks or controls the intelligence assets, what they are tasked to provide, and for what purpose they are tasked. ES is achieved by **intelligence collection, processing, and exploitation assets** tasked or controlled by an operational commander. These assets are tasked **to search for, intercept, identify, and locate or localize** sources of intentional or unintentional radiated EM energy. The purpose of ES tasking is **immediate threat recognition, targeting, planning and conduct of future operations**, and other tactical actions such as threat

avoidance, targeting, and homing. ES is intended to respond to an **immediate operational requirement**. However, the same assets and resources that are tasked with ES can simultaneously collect intelligence that meets other collection requirements. Intelligence collected for ES purposes is normally also processed by the appropriate parts of the intelligence community for further exploitation after the operational commander's ES requirements are met.

9. Service Perspectives of EW

Planning and execution of joint EW is affected by the different viewpoints on EW held by the Military Services. Although formal EW definitions are standardized in the Department of Defense (DOD), different operational environments and tactical objectives lead to variations in perspective among the Services.

Appendix F, "Service Perspectives of Electronic Warfare," gives a brief overview of the differences in EW perspective among the four Services.

CHAPTER II

ORGANIZING FOR JOINT ELECTRONIC WARFARE

“Generally, management of the many is the same as management of the few. It is a matter of organization.”

Sun Tzu

1. Introduction

How joint forces are organized to plan and execute EW is a **prerogative of the JFC**. The size of the commander’s staff, the mission or missions which the joint force is tasked to accomplish, and the time allocated to accomplish the mission or missions are just some of the factors which affect the organization of the staff. This chapter discusses the nominal **organization of staff functions** to plan and execute EW in joint operations. It also summarizes EM spectrum management functions and the joint level organization of intelligence support to EW. A brief introduction to **how each of the four Services is organized to plan and execute EW** is provided in order to give an understanding of how joint staff EW functions interact with Service components.

2. Joint EW Organization

EW has operational implications for planning and supervision functions that are normally divided among several directorates of a joint staff. **Long-range planning** of EW normally occurs under the **Plans Directorate (J-5)**. More **immediate planning and the supervision** of execution of EW normally falls within the purview of the **Operations Directorate (J-3)**. The EA portions of joint EW normally must be coordinated closely with joint force components and deconflicted with the Command, Control, Communications, and Computer Systems Directorate (J-6) and the Intelligence Directorate (J-2). The joint restricted frequency list (JRFL) is promulgated by the J-6 in coordination with the J-3. The EP

functions of joint EW affect and are affected by planning and activities within the J-2 and J-6. The ES and EA functions of EW require close cooperation between the J-2 and the J-3.

a. **J-3.** Authority for planning and supervising joint EW is normally **delegated by the JFC to the J-3**. When so authorized, the J-3 will have primary staff responsibility for **planning, coordinating, integrating, and ensuring execution of joint force EW operations**. The J-3 may delegate staff responsibility for EW as appropriate for the size of the staff and scope of J-3 responsibilities.

b. **IO Officer.** The IO officer on a joint staff is responsible for **coordinating the constituent parts of IO** in the joint planning process. **Leadership of the “IO cell”** is normally one of the functions of the IO officer.

JP 3-13, “Joint Doctrine for Information Operations,” provides details about the organization and procedures of the IO cell.

c. **EW Officer.** Normally, the EW officer is the **principal staff EW planner** on a joint staff. The scope and nature of the EW officer’s responsibilities are dependent on the size of the staff, the operational area of the JFC that the staff supports, and the type of mission or operation that the staff must plan. The types of duties that may be assigned to the EW officer are shown in Figure II-1.

d. **EW Staff.** The requirement for staff personnel to support the EW officer varies among joint staffs. The number of personnel required to carry out EW staff functions, their

DUTIES ASSIGNED TO THE ELECTRONIC WARFARE OFFICER

PRIMARY:

Coordinating with tactical operations and the other members of the information operations (IO) cells.

SECONDARY:

Drafting and supervising the implementation of electronic warfare (EW) policies and instructions within the commander's operational area.

Serving as the command's principal delegate to EW planning and coordination meetings within the operational area.

Supervising EW planning efforts and the preparation of EW appendices to operation plans.

Coordinating the planning for and preparation of EW in joint exercises within the commander's operational area.

Monitoring the number, type, and status of US EW assets within the operational area or involved in specific operations or exercises.

Coordinating the augmentation of EW staff planners and EW assets for exercises and operations within the operational area.

Representing EW interests in the preparation of the joint restricted frequency list for specific operations and exercises within the operational area.

Coordinating the multinational aspects of EW in exercises and operations within the operational area.

Representing EW interests and requirements in the IO cell and other multifunctional planning organizations within the staff.

Monitoring the execution of the EW plans in current operations and exercises within the operational area and supervising the adaptation of those plans to meet operational contingencies.

Monitoring EW reprogramming requirements within the operational area and making recommendations for reprogramming when appropriate.

Coordinating and supervising the analysis of EW plans and activities during operations and exercises within the operational area in order to derive lessons learned.

Supervising the preparation and submission of EW lessons learned in accordance with the Joint After-Action Reporting System.

Figure II-1. Duties Assigned to the Electronic Warfare Officer

areas of expertise, and the division of labor among them should be appropriate to the scope of the commander's responsibilities.

3. Joint EW Staff Manning

The integration of the concepts of IO in joint doctrine formalized the requirements for EW

coordination within the joint staff. On many joint staffs, the intra-staff coordination previously accomplished through a "joint commander's electronic warfare staff" has now been replaced by the functions of an "IO cell" or similar organization. Despite this trend, EW remains a sophisticated and technically complex aspect of military

operations that requires detailed staff planning and coordination. Accomplishment of this work requires that the core members of a staff assisting the EW officer have a **depth of technical expertise and knowledge** of the capabilities of EW systems currently employed by components, allies, and coalition partners. **Augmentation of joint staffs** during times of crisis or impending operations to accumulate additional EW expertise is almost always necessary. However, augmentees may have limited joint experience and require time to be trained in joint staff procedures. Innovative staffing solutions may be necessary if the number of billets assigned specifically to EW planners falls short of the requirements necessary to accomplish EW staff work. During crisis action planning (CAP), permanent joint staffs, such as combatant commander staffs, may consider requesting that components provide augmentees with the necessary technical expertise to be assigned to assist the permanent members of the joint staff on a temporary basis. Assignment of allied exchange personnel that have a background in EW is also a possible solution to EW staffing shortfalls on permanent joint staffs. Joint staffs that are organized to carry out specific operations should seek to identify specific EW staff manning requirements early on in the process of standing up a joint task force (JTF) or other temporary joint staff. Where feasible, manning requests to fill EW billets on contingency joint staffs should emphasize the need to fill such billets with personnel experienced in joint operation planning as well as the requisite EW expertise.

4. Joint Frequency Management Organization

Each geographic combatant commander is specifically tasked by joint EM spectrum use policy (Chairman of the Joint Chiefs of Staff Instruction [CJCSI] 3220.01, “Electromagnetic Spectrum Use in Joint

Military Operations”) to establish a frequency management structure that includes a **joint frequency management office (JFMO)** and to **establish procedures** to support planned and ongoing operations. The supported combatant commander authorizes and controls use of the spectrum resources by the military forces under his or her command. Each supported combatant commander establishes a command policy on how the spectrum is used in their operational area, obtains clearance (or approval) from host nations for use of the spectrum (through existing coordination procedures), and ensures that assigned military forces are authorized sufficient use of the spectrum to execute their designated missions. To accomplish these tasks, each supported combatant commander establishes a JFMO, typically under the cognizance of the J-6, to **support joint planning, coordination, and control of the spectrum** for assigned forces. The JFMO may be assigned from the supported combatant commander’s J-6 staff, from a component’s staff, or from an external command such as the Joint Spectrum Center (see Appendix C, “Joint Spectrum Center Support to Joint Electronic Warfare”). In any event, the JFMO must be staffed with trained spectrum managers, preferably with experience in joint spectrum use and knowledge of the spectrum requirements of the combatant command component forces. Figure III-1 diagrams the spectrum management process followed by the JFMO.

The basic process the JFMO uses to carry out its primary responsibilities is discussed further in Chapter III, “Planning Joint Electronic Warfare,” and Chapter IV, “Coordinating Joint Electronic Warfare.” Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3220.01, “Joint Operations in the Electromagnetic Battlespace,” provides additional information about the JFMO and its functions and processes.

5. Organization of Intelligence Support to EW

The intelligence community is organized into **three levels to provide intelligence support** to joint military operations (see Figure II-2). Each of these levels is closely and continuously involved in providing support for EW.

a. **National-Level Intelligence Organizations.** At the national level, organizations and agencies such as the Central Intelligence Agency (CIA), National Security Agency (NSA) and Defense Intelligence Agency (DIA) are constantly seeking to

identify, catalog, and update the electronic order of battle (EOB) of identified or potential adversaries. Other intelligence agencies, such as the National Imagery and Mapping Agency (NIMA), **support the maintenance of the EOB.** National-level organizations also **analyze and provide intelligence on adversary EW doctrine and tactics.** National-level collection efforts also provide much of the intelligence that is gathered about adversary electronic infrastructures. The DIA J-2 National Military Joint Intelligence Center (NMJIC) is the focal point for tasking national assets to collect EW in response to intelligence requirements. EW intelligence requirements that cannot be met



Figure II-2. Organization of Intelligence Support to Electronic Warfare

by lower-level intelligence assets are forwarded to NMJIC for prioritization and tasking to national assets.

JP 2-02, “National Intelligence Support to Joint Operations,” provides more detailed discussion on the organization of national-level intelligence support.

b. Combatant Command. At the combatant command level, intelligence support to military operations is focused in the **Joint Intelligence Center (JIC)**. The JIC responds to theater-level EW intelligence requirements and forwards requests that require national-level assets to the NMJIC or other national-level organization according to established procedures. EW planners at the combatant command level work with the command J-2 staff to **satisfy EW intelligence requirements** according to command-specific procedures established by each commander of a combatant command (CINC).

JP 2-0, “Doctrine for Intelligence Support to Joint Operations,” provides additional discussion of how theater-level intelligence support is accomplished.

c. Subordinate Joint Force. The J-2 is the **primary point of contact** for providing intelligence support to joint EW. Within the context of a geographic combatant command, individual subordinate joint force J-2 organizational structures will be situation- and mission-dependent, as determined by the JFC. The J-2 normally assigns one or more members of their staff to act as a liaison between the J-2 section of the staff and the IO cell (or other IO staff structure) where EW planners are normally assigned. At the discretion of the JFC, a **joint intelligence support element (JISE)** is established either during crisis or the preparation stage for operations in order to augment the subordinate joint force J-2 element. Under the direction of the joint force J-2, a JISE normally

manages the intelligence collection, production, and dissemination of a joint force. The purpose of this liaison is to coordinate collection requirements and analytical support for compartmented and non-compartmented IO. Because of the close interrelationship between EW (particularly ES) and activities such as SIGINT, EW planners may find it necessary to work with a wide variety of personnel in the intelligence section of the staff.

JP 2-01, “Joint Intelligence Support to Military Operations,” discusses how the intelligence community is organized to support joint military operations.

6. Service Organization for EW

Each Military Service has a different approach to organizing their forces in order to plan and execute EW. Since the Services provide most US EW assets, a basic understanding of each Service’s EW organization greatly facilitates the planning and coordination of EW at the joint level.

a. Army. Army EW assets are organized to ensure that EW operations are developed and integrated as part of the commander’s overall concept of operations. At each echelon of Army organization responsible for an EW mission, the **IO cell officer in charge (OIC), under the direction of the component operations staff officer (G-3) or battalion or brigade operations staff officer (S-3) is responsible for planning and coordinating** EW operations into the IO plan. The **electronic warfare officer (EWO)** is responsible to the G-3 and coordinates with the IO cell OIC and the component command, control, communications, and computer systems staff officer (G-6) for planning, synchronizing, coordinating, and deconflicting EW actions. The EWO normally works closely with the **fire support coordinator** to integrate EW efforts with other supporting fire missions. The **EW**

coordination center (EWCC) is an ad hoc staff coordination element often formed to facilitate the EW coordination function.

b. **Marine Corps. Marine EW assets are integral to the Marine air-ground task force (MAGTF).** The G-3 or S-3 has staff responsibility for planning and coordinating MAGTF EW operations and activities. Ground-based EW is provided by the radio battalion (RADBN), and airborne EW is provided by Marine tactical EW squadrons (VMAQs). The RADBN is organized and equipped to conduct tactical SIGINT, ground-based ES, communications EA, and communications security (COMSEC) monitoring and analysis in support of the MAGTF. To accomplish this mission, the RADBN provides the MAGTF with task-organized detachments. VMAQs conduct ELINT operations as well as EA, ES, and EP training in support of aviation and ground units. With the employment of both the RADBN and the EA-6B aircraft in combination with the Marine Corps' Tactical Electronic Reconnaissance Processing and Evaluation System, the Marine Corps possesses a unique capability to provide **EW support and SIGINT to the MAGTF commander and any subordinate elements** while also providing invaluable support and information to the JFC. The MAGTF commander will normally plan, synchronize, coordinate, and deconflict EW operations through an EWCC.

For more information about EA-6B employment, see the Air Land Sea Application Center publication "Multiservice Tactics, Techniques, and Procedures for EA-6B Employment in the Joint Environment." This publication is referenced Service-wide as Field Manual (FM) 90-39, Marine Corps Reference Publication (MCRP) 3-22A, Naval Warfare Publication (NWP) 3-01.4, and Air Force Tactics, Techniques, and Procedures (Interservice) (AFTTP[I]) 3-2.4.

c. **Navy.** Naval forces are normally organized to support joint operations according to the **composite warfare commander (CWC) concept**. Within this concept, the information warfare commander (IWC) is responsible for the **integration of the various elements and activities of IO**, including EW, into naval and joint operations. An EWO is normally assigned to the IWC's staff to carry out specific staff coordination and integration functions associated with EW's role in the IO effort. EW is planned and conducted by the EWO under the direction of the IWC. The IWC watch oversees the execution of the coherent EW and IO plan and control of associated systems. Control of the ES and non-communications portion of the plan requires continual monitoring by EW staff personnel and is delegated to the EW control ship.

NOTE: The functions of the IWC are primarily defensive in nature, coordinating IO for the defense of the battle group. Embarked airborne EA assets, such as the EA-6B Prowler, are under the operational control of the strike warfare commander, who is also the carrier battle group air wing commander (CVWC) or the more traditional "carrier air group" (CAG). When executing strike operations, air wing EA assets will remain under the operational control of the CAG, and will come under the tactical control of the airborne mission commander. When assigned to joint or coalition operations, the joint force air component commander (JFACC) will coordinate with CAG operations for scheduling air wing assets in the air tasking order (ATO). When airborne assets are assigned ashore as part of an expeditionary force, they will be transferred to the operational control of the JFACC. It should also be noted that Navy airborne ES is primarily provided by shore-based aircraft such as the EP-3E Aries II. These aircraft will come under the operational control of the theater maritime and reconnaissance task force commander, and will be assigned to the

tactical control of either the battle group IWC or the JFACC as scheduled by the ATO.

d. **Air Force.** Within the Air Force component, dedicated EW support assets are under operational control of the **Commander, Air Force Forces (COMAFFOR)**. Within the COMAFFOR headquarters, the office of primary responsibility for EW is the Operations Directorate (A-3) and Plans Directorate (A-5). **Functional planning, directing, and control of Air Force EW assets, however, are normally conducted by the JFACC** through the joint air operations center's Director and its Information Warfare Team, by means of the ATO. In response to the ATO, wing and unit level staffs and individual aircrews develop the detailed tactical planning for specific EW missions.

Due to the high demand for support from Air Force dedicated tactical systems, these systems are normally organized as separate EW wings and squadrons, whose employment the JFACC carefully rations through the ATO process. Air Force EP and ES systems, however, are normally assigned to or integrated into Air Force wings or squadrons. Wing commanders are supported by a staff defensive systems officer (DSO), EWO, or electronic combat officer (ECO). These officers work with the wing operations intelligence staff to analyze and evaluate the threat in the theater or operational area. The DSO, EWO, and ECO also plan available EW equipment employment and oversee radar warning receiver and EW systems reprogramming.

Intentionally Blank

CHAPTER III

PLANNING JOINT ELECTRONIC WARFARE

"...the most important single outcome of technological progress during the decades since World War II has been that, on the modern battlefield, a blizzard of electromagnetic blips is increasingly being superimposed on, and to some extent substituted for, the storm of steel in which war used to take place."

Martin Van Creveld
Technology and War, 1989

1. Introduction

a. EW is a complex aspect of modern military operations that must be **fully integrated** with other aspects of joint operations in order to achieve its full potential for contributing to an operation's objectives. Such integration requires **careful planning**. EW planners must be concerned with **coordinating their planned activities with other aspects of military operations** which use the EM spectrum as well as third party users of the spectrum that EW does not wish to disrupt. Coordination of military use of the spectrum is largely a matter of coordinating with other staff functions (primarily the J-2 and J-6 as well as the other elements of IO, such as PSYOP planners) and components (to include allies and coalition partners) which rely on the EM spectrum to accomplish their mission. Coordination of EW activities in the context of third party use of the EM spectrum is largely a matter of EM spectrum management and adherence to established frequency usage regimens and protocols.

b. Like other aspects of joint operations, joint EW is **centrally planned and decentrally executed**. Since the Military Services provide most US EW assets available in joint operations, **Service component EW planners must be integrated into the joint planning process**. The JFC may delegate control of EW operations to a component commander or lower echelon. However, such

delegation does not eliminate the requirement for joint and/or multinational coordination of EW operations. This chapter provides guidance on the joint EW planning process, discusses some of the considerations that must be taken into account when planning EW in support of military operations, provides guidance on preparation of the EW portion of the operation plan (OPLAN) and/or operation order (OPORD), and briefly discusses some of the automated decision aids that may be used to assist with planning joint EW.

2. EW Planning Considerations

a. **EM Spectrum Management.** Since EW activity takes place in the EM spectrum, joint **EW planners must closely coordinate their efforts** with those members of the joint staff who are concerned with managing military use of the EM spectrum. Figure III-1 shows the steps involved in JFMO spectrum management responsibilities. Figure III-2 shows a flow diagram of frequency management planning. For operations within a CINC's operational area, the subordinate JFCs follow this guidance as amplified by the CINC. The commander, JTF coordinates and negotiates modifications necessary for a specific JTF situation with the CINC's staff. For operations outside a CINC's operational area, JFCs assume the spectrum management responsibilities of the CINC. Joint EW planners should establish and maintain a close working relationship with the frequency

JOINT FREQUENCY MANAGEMENT OFFICE SPECTRUM MANAGEMENT PROCESS

1. Develops and distributes spectrum-use plans that include frequency reuse and sharing schemes for specific frequency bands, as appropriate. This is particularly vital in support of command and control hand-overs that are highly dependent on radio systems.
2. In conjunction with the J-2, J-3, and J-6, prepares a joint restricted frequency list (JRFL) for approval by the J-3 (through the information operations [IO] cell or equivalent).
3. Periodically updates and distributes the JRFL, as necessitated by changes in the task organization, geography, and joint communications-electronics operation instructions and by transition through operational phases.
4. Provides administrative and technical support for military spectrum use.
5. Exercises frequency allotment and assignment authority. This may be delegated to facilitate decentralization and to provide components with the maximum latitude and flexibility in support of combat operations.
6. Establishes and maintains the common data base necessary for planning, coordinating, and controlling spectrum use. This data base should contain spectrum-use information on all emitters and receivers (critical, friendly, military and civilian, available enemy, and neutral) as appropriate for the area of responsibility involved.
7. Analyzes and evaluates potential spectrum-use conflicts.
8. As a member of the IO cell (or equivalent), assists and coordinates the resolution of spectrum-use conflicts.
9. In accordance with J-5 guidance, coordinates military spectrum use with the spectrum authorities of the United Nations or host nations involved.
10. Serves as the focal point for inclusion of spectrum-use considerations in the Joint Operation Planning and Execution System.
11. Receives, reports on, analyzes, and attempts to resolve incidents of unacceptable electromagnetic interference; refers incidents that cannot be resolved to the next higher spectrum management authority.
12. Functions as a member of the IO cell by performing steps 2, 3, 4, 7, 8, and 11.

Figure III-1. Joint Frequency Management Office Spectrum Management Process

management personnel. **The JRFL is a critical management tool** in the effective use of the EM spectrum during military operations. Normally the J-6 is responsible for promulgating the JRFL, but the J-3 is responsible for coordination of the preparation of the JRFL during operation planning. The

EWO within the IO cell is normally delegated the responsibility for coordinating the preparation of the JRFL. The Joint Spectrum Center (JSC) can support this responsibility, including provision of automated frequency management tools and augmentation personnel to assist with JRFL preparation and

JOINT TASK FORCE ELECTROMAGNETIC SPECTRUM MANAGEMENT PLANNING FLOW

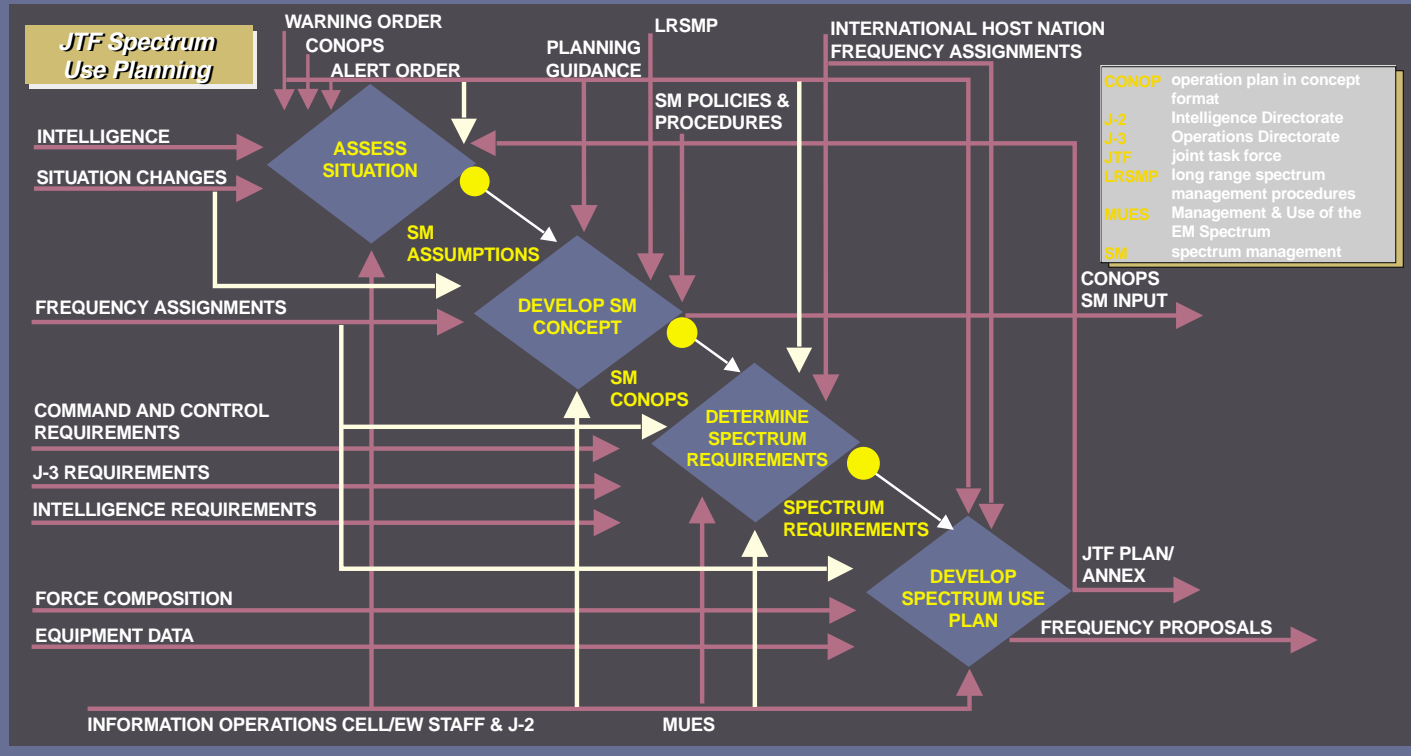


Figure III-2. Joint Task Force Electromagnetic Spectrum Management Planning Flow

other frequency management tasks. EW planners should **coordinate with J-6 and J-2 personnel** and request assistance from the JSC early in the planning process.

See Appendix B, “Electronic Warfare Frequency Deconfliction Procedures,” for frequency deconfliction procedures and information on generating the JRFL.

For exercises conducted in the US or Canada, EW planners must consult CJCSM 3212.02, “Performing Electronic Attack in the United States and Canada,” for planning and guidance procedures.

CJCSM 3220.01, “Joint Operations in the Electromagnetic Battlespace,” provides more detailed guidance in EM spectrum management. For more information on the JSC, see Appendix C, “Joint Spectrum Center Support to Joint Electronic Warfare.”

b. **EW as a Part of IO.** EM energy is the means by which **modern information systems process and store information**. EM energy is also used for **sensing, measuring, analyzing, and communicating** information. This dependence on EM energy and use of the EM spectrum by the systems that sense,

process, store, measure, analyze, and communicate information create **IO opportunities and vulnerabilities** that EW can address. EA tactics, techniques and procedures from a variety of EW platforms can offer a range of lethal and nonlethal options to affect adversary information and information systems. EP tactics, techniques, and procedures are essential to **protecting friendly information and information systems**. ES is a primary means for **gathering information** during joint operations. All EW activities conducted as part of or in support of joint operations should be **coordinated through the IO cell** of the joint staff in order to realize the potential synergistic benefit of synchronizing the efforts of all the capabilities and related activities of IO in a coordinated manner.

c. **EW Support of SEAD.** SEAD is a specific type of mission intended to **neutralize, destroy, or temporarily degrade** surface-based adversary air defenses with destructive and/or disruptive means. Joint SEAD is a broad term that includes **all SEAD activities** provided by one component of the joint force in support of another. SEAD missions are of critical importance to the success of any joint operation when control



SEAD missions are of critical importance to the success of any joint operation when control of the air is contested by an adversary.

of the air is contested by an adversary. SEAD relies on a variety of EW platforms to conduct ES, EP, and EA in support, and EW planners should coordinate closely with joint and component air planners to ensure that EW support to **SEAD missions is integrated into** the overall EW plan.

For more information about SEAD, see JP 3-01.4, “Joint Tactics, Techniques, and Procedures for Joint Suppression of Enemy Air Defenses (J-SEAD).”

d. **EW Reprogramming.** The purpose of EW reprogramming is **to maintain or enhance the effectiveness of EW and TSS equipment.** EW reprogramming includes **changes to self-defense systems, offensive weapons systems, and intelligence collection systems.** The reprogramming of EW and TSS equipment is the responsibility of each Service or organization through its respective EW reprogramming support programs. However, during joint operations, the swift identification and turnaround of reprogramming efforts could become a matter of life and death in a rapidly evolving hostile situation. Service reprogramming efforts must include coordination with JFCs to ensure that those reprogramming requirements are identified, processed, and implemented in a timely manner by all affected friendly forces.

See Appendix D, “Electronic Warfare Reprogramming,” for more information about reprogramming.

e. **Electronic Masking**

- Electronic masking is the **controlled radiation of EM energy on friendly frequencies** in a manner to protect the emissions of friendly communications and electronic systems against adversary ES and SIGINT without significantly degrading the operation of friendly systems. Electronic masking is used to **disguise, distort, or manipulate**

friendly sensor-related data to conceal military operations information and/or present false perceptions to adversary commanders. Electronic masking is an **important component to a variety of military functions** (such as EW, camouflage, military deception, OPSEC, and signals security) that are conducted, wholly or in part, within the EM spectrum.

- Effective electronic masking of joint military operations involves the proactive management of all friendly radiated electronic signatures of equipment being used in or supporting the operation. The **degree of masking required** in the management of these signatures is a function of two variables:
 - the assessed adversary ES and SIGINT collection capability (or access to third party collection); and
 - the degree to which the electronic signature of joint forces must be masked in order to accomplish the assigned mission.
- JFCs have **two primary responsibilities** with respect to electronic masking:
 - providing adequate electronic masking guidance to component commands through OPLANs and OPORDs; and
 - planning and implementing appropriate electronic masking measures within the joint force headquarters.
- To accomplish these responsibilities, the **following steps should be taken early** in the planning process:
 - Assess the adversary ES and SIGINT capabilities against friendly forces;

- Determine whether the mission assigned to joint forces may require electronic masking and, if so, to what degree;

- Request staff augmentation if necessary to acquire expertise in planning and implementing electronic masking tactics, techniques, and procedures; and

- Alert component commands at the earliest opportunity of the need to be prepared to implement electronic masking measures. This will afford these commands with the necessary lead time to augment their own forces with the necessary resources and expertise.

f. **Interoperability.** Interoperability is essential in order to use EW effectively as an element of joint military power. The major requirements of interoperability are:

- to **establish standards and practice procedures** that allow for integrated planning and execution of EW operations (including joint EW); and
- to **exchange EW information in a timely and routine fashion.**

This exchange may be conducted in either non real time or in near real time via common, secure, jam-resistant radios and data links. The ability to **exchange near real time data (such as targeting information) enhances situational awareness and combat coordination** between various force elements, including EW strike and/or execution assets, command-control units, ES collection units, supported units, and others, is a critical combat requirement. This exchange of data relates to ES, EA, and EP, including friendly and adversary force data. Routine exchange of data among joint force components, the joint force and supporting commands and organizations and, when

possible, with allies and coalition partners greatly facilitates all types of EW planning.

g. **Rules of Engagement.** EW activities frequently involve a unique set of complex issues. There are federal laws, federal agency publications and directives, laws of armed conflict (LOACs), and theater rules of engagement (ROE) that may affect EW activities. These guidelines become especially critical during sensitive peacetime operations when international and domestic laws, treaty provisions, and political agreements may affect mission planning and execution. Commanders must seek legal review during all levels of planning and execution of EW activities, to include planning of the theater ROE. This can best be accomplished by having a legal advisor as a member of the IO cell.

3. Joint EW Planning Process

Like other aspects of joint operations, **joint EW planning is conducted through the Joint Operation Planning and Execution System (JOPES) process.** In order to be fully integrated into other aspects of a planned operation, EW planning must start in the earliest stages of the JOPES process and be coordinated with other aspects of the plan every step of the way. Figures III-3 and III-4 show the integration of EW into both the JOPES deliberate and crisis action planning process, respectively. Once a planned operation has commenced, EW planners must **monitor execution of the plan** and be prepared to **assist with coordination** of the plan as well as make modifications to the plan as the dynamics of the operation evolve. Joint EW planners should take the following actions during the planning process to **integrate EW into the joint plan.**

- a. Determine the type, expected length, geographic location, and level of hostility expected during the operation to be planned.

ELECTRONIC WARFARE PLANNING RELATED TO DELIBERATE PLANNING

PLANNING PHASE	JOPEs	EW PLANNING ACTION	EW PLANNING OUTCOME
PHASE I	Initiation	Notify EW planners of planning requirements. Request augmentation of EW planning staff as required.	EW planner augmentation if necessary.
PHASE II	Concept Development		
Step 1	Mission Analysis	EW planners identify information requirements needed for mission planning.	Tasking to gather and obtain required information.
Step 2	Planning Guidance	EW planners assist in development of CINC's planning guidance to support overall operational planning guidance.	EW incorporated into CINC's planning guidance.
Step 3	Staff Estimates	EW planners support the development of intelligence, operations, and communications staff estimates.	EW incorporated into staff estimates.
Step 4	CINC's Estimate	EW planners assist in transforming staff estimates into the CINC's Estimate.	EW incorporated into CINC's Estimate.
Step 5	CINC's Concept	EW planners assist in development of CINC's Concept as required.	EW incorporated into CINC's Concept.
Step 6	CJCS Concept Review	EW planners assist in the CJCS Concept Review as required.	EW aspects of operational concept approved by Chairman.
PHASE III	Plan Development	EW planners develop the EW portion of the IO plan and assist in development of other sections as appropriate in coordination with other staff sections, operational units, and supporting agencies.	Draft EW tab to IO appendix and integration of EW considerations into other sections of OPLAN as appropriate.
PHASE IV	Plan Review	EW planners modify or refine EW portions of plan as necessary.	Approved EW tab to IO appendix and integration of EW considerations into other appropriate sections of the OPLAN.
PHASE V	Supporting Plans	Subordinate units and supporting agencies prepare their own EW plans. Joint EW planners coordinate or assist subordinate and supporting EW plans as necessary. Ensure that TPFDD supports EW portions of plan.	Completed subordinated and supporting agencies' supporting plans. EW portions of plan supported by TPFDD.
CINC Combatant Commander JOPEs Joint Operation Planning and Execution System CJCS Chairman of the Joint Chiefs of Staff OPLAN Operation Plan EW Electronic Warfare TPFDD Time-Phased Force and Deployment Data IO Information Operations			

Figure III-3. Electronic Warfare Planning Related to Deliberate Planning

b. Review the scale of anticipated operations and the number and type of friendly forces (to include allied and coalition partners) expected to participate. in accordance with current staff procedures. Coordinate with legal to ensure that requirements of the LOAC are met.

c. Review current ROE on EW activities and recommend any necessary modifications

d. Review the contribution which EW can make to the IO effort with other “element level” planners (such as PSYOP and military

ELECTRONIC WARFARE PLANNING RELATED TO CRISIS ACTION PLANNING

PLANNING PHASE	JOPEs	EW PLANNING ACTION	EW PLANNING OUTCOME
PHASE I	Situation Development	Monitor situation. EW planners identify planning information requirements as situation develops. Review applicable CONPLAN. Request augmentation of EW planning staff as required.	Tasking to gather and obtain required information. EW planner augmentation if necessary.
PHASE II	Crisis Assessment	EW planners continue to identify emerging information requirements needed for mission planning. Assist in development of CINC's planning guidance to support overall operational planning guidance.	EW incorporated into CINC's planning guidance. Initial liaison with units and agencies that may participate in or support EW during operation.
PHASE III	COA Development	EW planners support the development of intelligence, operations, and communications staff estimates for each COA.	EW incorporated into staff estimates for each COA.
PHASE IV	COA Selection	EW planners transforming EW aspects of staff estimates associated with selected COA into CINC's Estimate. Assist with EW aspects of CINC's Concept as required.	EW aspects of operational concept approved through the Chairman of the Joint Chiefs of Staff.
PHASE V	Execution Planning	EW planners develop EW tab to IO plan and assist in development of EW aspects of other sections as appropriate in coordination with other staff sections, operational units, and supporting agencies.	Approved EW tab to IO appendix and integration of EW considerations into other appropriate sections of the OPLAN. Completed subordinate and supporting agencies' supporting plans. EW portions of plan supported by TPFDD.
PHASE VI	Execution	Joint EW planners monitor EW aspects of operations and coordinate adaptation of EW plans, procedures, and resources to support changing operational directives.	EW plans, procedures, and resources adapted to changing operational requirements.

CINC	Combatant Commander	IO	Information Operations
CJCS	Chairman of the Joint Chiefs of Staff	JOPEs	Joint Operation Planning and Execution System
COA	Course of Action	OPLAN	Operation Plan
CONPLAN	Operation Plan in Concept Format	TPFDD	Time-Phased Force and Deployment Data
EW	Electronic Warfare		

Figure III-4. Electronic Warfare Planning Related to Crisis Action Planning

deception planners) and determine what level of EW platform support they expect to need during the operation.

e. Review with intelligence planners the type of ES platforms and products available to support the operation.

f. Consult with Service and functional components as well as multinational EW planners, wherever the most current expertise in the capabilities and employment of EW platforms resides, in order to understand the full range of capabilities that EW can contribute to IO.

g. Determine the number and type of EW platforms that could reasonably be expected to be tasked to support the joint operation being planned. Consult automated force status reports (such as those provided through the Status of Readiness and Training System for US forces) for this information. Service and functional components and multinational planners should be consulted to augment automated information.

h. Review with component air planners the requirement for EW support to the SEAD effort.

i. Recommend to the IO officer (or other designated member of the J-3 or J-5 staff) the type and number of EW assets to be requested from component or supporting commands for the operation being planned.

j. Estimate the size and expertise of the EW staff required to plan and coordinate execution of the EW portion of the plan. Consult Service and functional component and multinational EW planners to refine these estimates.

k. Recommend staff augmentation in accordance with staff procedures from component, supporting, and multinational forces as necessary to assemble the necessary staff to conduct EW planning.

l. Request assistance and augmentation as necessary from the JSC to assist with preparation of the JRFL and other EM spectrum management tasks.

m. During CAP, evaluate each COA considered with respect to EW resources required and the EW opportunities and vulnerabilities inherent in the COA.

4. EW Planning Guidance

Planning guidance for EW should be **included in an OPLAN** as a tab to the IO

guidance. IO guidance is normally appended to Annex C of the OPLAN.

Appendix A, “JOPES Electronic Warfare Guidance,” shows the format of JOPES EW guidance as a tab to the IO guidance. CJCSM 3122.03, “Joint Operation Planning and Execution System Vol II: (Planning Formats and Guidance)” and its classified supplement, CJCSM 3122.04, “Joint Operation Planning and Execution System Vol II: (Supplemental Planning and Execution Formats and Guidance)” are the source documents that should be consulted for detailed information about OPLAN development.

a. **Planning Factors.** Development of the EW portion of the OPLAN requires consideration of a number of diverse factors about the proposed operations. Some of these **planning factors** include the following.

- **Requirements for friendly communications nets, EM navigation systems, and radar.** These requirements should be considered with respect to the anticipated operations, tactical threat expected, and EM interference considerations. Once identified, these requirements should be entered into the JRFL under appropriate categories (e.g., TABOO).
- **Identification of COMSEC and electronic security measures necessary to deny OPSEC indicators to enemy passive-EM sensors.**
- **Determination of what prior coordination and precautions will be necessary when conducting EA in order to ensure continued effective ES.** Development of the JRFL is a critical preliminary step to ensuring deconfliction of EA and ES activities.

- Coordination and identification of specific resources required for interference deconfliction.
 - Identification of commander's critical information requirements (CCIR) that support commanders and EW operations. These CCIR must be included in the intelligence annex (normally Annex B) of the OPLAN to facilitate generation of ES.
 - Coordination and establishment of procedures to ensure timely fulfillment, including tactical real-time dissemination.
 - Review of ROE to determine what restrictions (if any) apply to EW operations.
- b. **EW plans should:**
- **Identify the desired EM profile** selected by the commander for the basic concept of operations and **provide EMCON guidance** to commanders so that desired EM and acoustic profiles are realized;
 - **Identify EW resources** required to support IO, SEAD, and other activities; and
 - **Evaluate enemy threats** to critical friendly C2 communications, weapons control systems, target acquisition systems, surveillance systems, and computer networks. Specify EP measures necessary to ensure effective operations during combat.
- a. **Databases.** Automated databases can assist EW planners by **providing easy access to a wide variety of platform-specific technical data** used in assessing the EW threat and planning appropriate friendly responses to that threat. However, planners should keep **several considerations** in mind when relying on automated data.
- There are a **large number of databases** available to military planners. Some of these databases are maintained by the Services, others by various intelligence community agencies or other DOD organizations, others by allied organizations. Still other databases may be maintained by academic or private (profit or non-profit) organizations. In general, **friendly data is maintained by Service, government contractor and allied organizations. "Threat" data is compiled by intelligence organizations.** Compilation of accurate technical data into one place is a lucrative target for hostile intelligence collection. For this reason, **access to friendly force data may be highly restricted** and harder for planners to obtain than threat data which can be accessed through normal intelligence channels.
 - The **level of detail, specific fields, and frequency of update** may vary widely across different databases dealing with the same data. The way that data is organized into fields in a database and the level of detail (such as number of decimal places certain technical data is carried out) are functions of what the data is used for and the cost associated with compiling and maintaining each database.
 - The sources of data being used for planning should be a topic of coordination among EW planners. If necessary, joint planners should provide guidance about what sources of

5. EW Planning Aids

There are a number of **automated planning tools** available to help joint EW planners carry out their responsibilities. These tools can be divided into three broad categories; **databases, planning process aids, and graphics analysis tools.**

automated data should be used for specific EW planning purposes. Planners should request that organizations that maintain important sources of EW data update their databases (or specific parts of them) more frequently than normal when planning specific operations. Planners should be cautioned about using unofficial sources of data, particularly those available through the Internet that may be subject to manipulation by organizations hostile to US policies and objectives. However, **open-source intelligence** remains a viable and important source of valuable information.

b. **Planning Process Aids.** There are **several automated aids** available that assist in the planning process and others under development. These include aids that **automate the JOPES planning process or OPLAN development, automated frequency management tools**, and others that assist with the **integration of different elements and activities of IO**. The type of automated software used in the JOPES planning process or OPLAN development will probably be directed by some other section of the staff. Use of automated tools to integrate different elements of IO will normally be determined by the IO officer. EW planners should ensure that any EW planning input developed separately from such systems are created in a format that is compatible

(electronically transferable) to designated planning tools. EW planning input solicited from subordinate and supporting commands should specify the format of such input.

c. **Graphics Analysis Tools.** The variables that affect the propagation of EM energy are known and **subject to mathematical predictability**. The use of automated analysis tools **that graphically display transmission paths** of such energy have become widespread in EW planning. However, the accuracy, speed, and flexibility of these tools greatly depend on the accuracy of the data provided to the tool and the sophistication of the software and hardware used to manipulate the data. Reliance on the output of such tools can ultimately be a matter of life and death in combat if the tools are used to plan the location of EW assets or avoid hostile emitters. These tools are essentially **models for EM propagation**. The accuracy and sophistication of the software and hardware being used may not be determined from the graphics display alone. **EW planners should have an understanding of how such modeling systems are computing the graphics being displayed.** Such an understanding, combined with operational experience, is the basis on which planners must rely to judge the strengths and weaknesses of different modeling tools and determine what is and is not an appropriate use of such systems.

Intentionally Blank

CHAPTER IV

COORDINATING JOINT ELECTRONIC WARFARE

"In the case of electronic warfare, as in any other kind of warfare, no weapon and no method is sufficient on its own."

Martin Van Creveld
Technology and War, 1989

1. Introduction

A certain amount of coordination is part of the planning process. However, once a plan has been approved and an operation is commenced, the preponderance of EW staff effort shifts to the coordination necessary to ensure that EW actions are carried out as planned or modified to respond to the dynamics of the operation. Areas of concern that normally require continual monitoring on the part of EW staff personnel include: **EW asset allocation, EM spectrum management, and emerging operational issues** that require modification to plans or procedures. Normally, such monitoring takes the form of **personnel on watch in the Joint Operations Center (JOC)**. Such watch personnel, stationed at an IO (or separate EW) watch station, normally are tasked to **alert other EW or staff personnel** to carry out specific coordinating actions in response to emerging requirements. This chapter discusses the actions and concerns on which EW staff personnel should focus to accomplish such coordination.

2. Joint Coordination and Control

a. **Management of the EM Spectrum.** The JFMO assessment of the operational area EME — conducted during the planning phase — constitutes a best guess based on information available at the time. Following deployment and buildup, overlaying joint force EM emissions on the existing operational area EME — during employment of the joint force — will create a new, and

somewhat different, actual environment. Further, this environment will constantly change as forces redeploy and as C2, surveillance, weapons systems, and other spectrum-use applications realign. Since EW is concerned with **disruption (EA), protection (EP), and monitoring (ES)** of the EM spectrum, EW staff personnel have a major role to perform in the **dynamic management** of the spectrum during operations. Figure IV-1 shows the execution of frequency use deconfliction during an operation. A **comprehensive and well thought out JRFL and EMCON plan** are normally the two tools that **permit flexibility of EW actions** during an operation without compromising friendly use of the EM spectrum. Some of the **coordination actions related to EM spectrum** that EW staff personnel should consider include:

- monitoring compliance with the JRFL and EMCON plan by friendly EW assets;
- recommending changes to EW operations based on emerging frequency deconfliction requirements;
- establishing ROE for EA employment, and ensuring that the EA plan is in compliance with the CINC's ROE;
- establishing a chattermark plan to ensure communications net availability in the presence of jamming, intrusion, or interference; and
- establishing and designating a jamming control authority (JCA) to conduct on-

EXECUTING WARTIME FREQUENCY USE

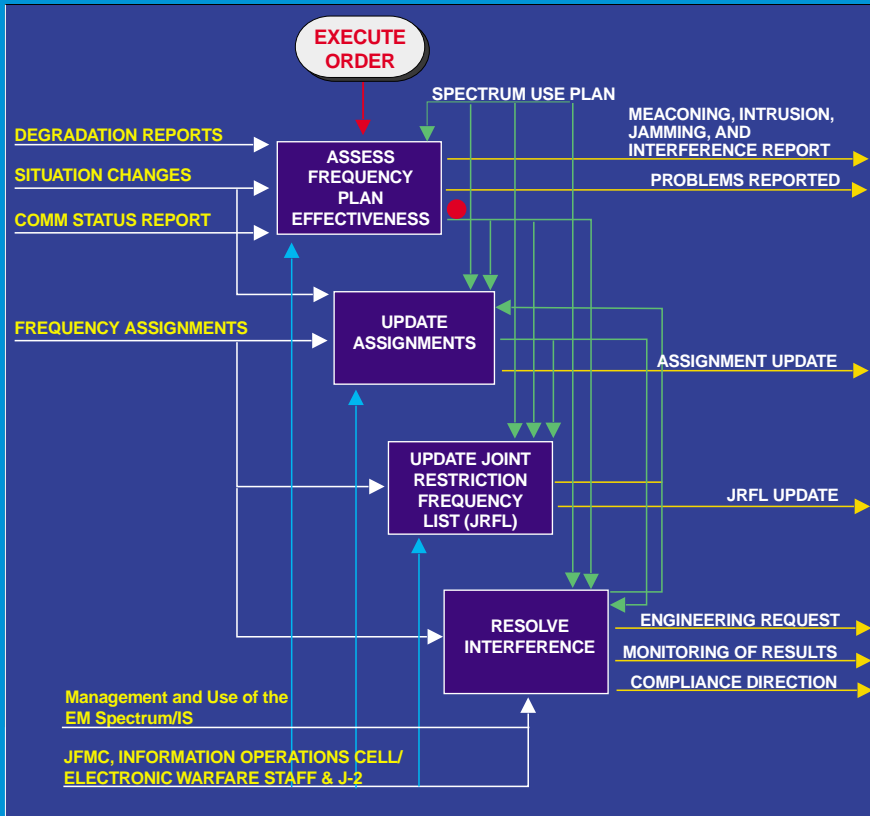


Figure IV-1. Executing Wartime Frequency Use

station coordination, employment, targeting, and deconfliction of EA and ES assets.

Paragraph 3 of this Chapter and Appendix B, “Electronic Warfare Frequency Deconfliction Procedures,” provide additional detail about EW frequency deconfliction.

b. Coordination Between the Subdivisions of EW. There are a number of **coordinating actions that must occur** among the respective divisions of EW (EA, EP, and ES) during an operation. These actions include:

- monitoring the employment and effective integration of ES assets and the timely flow of ES information relevant to EA and EP, to units responsible for those missions and coordinating corrective measures as required; and
- monitoring input to the reprogramming process submitted by components and coordinating urgent reprogramming actions on the basis of recommendations from Service reprogramming centers.

c. Coordination with the Other Elements and Activities of IO. One of the primary functions of the IO cell is to

deconflict and coordinate the various elements and activities of IO. Most of the elements and activities of IO depend on, use, or exploit the EM spectrum for at least some of their functions. The deconfliction and coordination of EW activities in an operation is a continuous process for the IO cell and EW staff personnel. Specific activities and concerns that must be **coordinated across IO elements and activities** are shown in Figure IV-2 and include the following.

- **PSYOP.** PSYOP are planned operations to **convey selected information and indicators** to foreign audiences to **influence their emotions, motives, objective reasoning and, ultimately, the behavior** of foreign governments, organizations, groups, and individuals. PSYOP activities often use the EM spectrum to broadcast their message to target audiences using platforms such as COMMANDO SOLO. EW activities support PSYOP and also have the potential to interfere with PSYOP efforts to convey information to adversaries or foreign target audiences. PSYOP platforms and units depend on information gathered through ES to **warn**

them of potential threats and provide feedback about reaction to PSYOP broadcasts and other activities. Jamming and other EA activities can potentially disrupt PSYOP broadcasts. PSYOP units rely on effective EP efforts to prevent adversary EA activities or other inadvertent EMI from disrupting their efforts. Coordination of PSYOP and EW planned frequency use when developing the JRFL is the first step in deconflicting these two activities. During the execution phase of an operation, PSYOP and EW staff personnel should deconflict their operations and frequency use on a regular basis.

JP 3-53, “Doctrine for Joint Psychological Operations,” provides additional detail.

- **OPSEC.** OPSEC is a process of **identifying critical information** and subsequently **analyzing friendly actions** attendant to military operations and other activities to:
 - identify those actions that can be observed by adversary intelligence systems;



PSYOP platforms and units depend on information gathered through ES to warn them of potential threats.

ELECTRONIC WARFARE ACTIVITIES COORDINATED WITH INFORMATION OPERATIONS ACTIVITIES

Psychological Operations (PSYOP): PSYOP are planned operations to convey selected information and indicators to foreign audiences.

Operations Security (OPSEC): OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities.

Military Deception: Military deception efforts can mislead adversary decision makers and slow or introduce error into their decisions. Knowledge of military deception plans and actions is normally very restricted. Forces assigned to the deception effort are often electronically "enhanced" to project a larger or different force structure to adversary sensors.

Physical Destruction: "Precision strike" is an increasingly important aspect of physical destruction actions in joint operations. Electronic warfare (EW) is an important part of precision strike. Factors require that joint EW staff personnel actively work with air planners, fire support personnel, and other staff personnel involved in coordinating the physical destruction actions during combat operations.

Computer Network Warfare: Computer Network Attack (CNA) and Computer Network Defense (CND). CNA and CND operations target and defend computer networks and systems. As many computer networks are linked electronically, incorporating the results of EW planning is crucial to both offensive and defensive computer network warfare campaigns. While physical access to a particular computer network may be limited, electronic access may prove the key to successful computer system penetrations.

Figure IV-2. Electronic Warfare Activities Coordinated With Information Operations Activities

• determine what indicators adversary intelligence systems might obtain that could be interpreted or pieced together

to derive critical information in time to be useful to adversaries; and

- select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.
- ES can support the OPSEC effort by providing information about adversary capabilities and intent to collect intelligence about **essential elements of friendly information (EEFI)** through the EM spectrum. ES can also be used to evaluate the effectiveness of friendly force EMCON measures and recommend modifications or improvements. An **effective and disciplined EMCON plan and other appropriate EP measures** are important aspects of good OPSEC. During operations, OPSEC planners and EW staff personnel should frequently review EEFI in light of the dynamics of the operation. Adjustments should be recommended to ES collection efforts, EMCON posture, and other EP measures as necessary to maintain effective OPSEC.

JP 3-54, “Joint Doctrine for Operations Security,” provides additional details.

- **Military Deception.** Military deception is defined as being those actions executed to **deliberately mislead adversary military decision makers** as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Knowledge of military deception plans and actions is normally very restricted. Designated EW staff personnel work through the IO cell to support and deconflict military deception with their own activities. Military deception frequently **relies on the EM spectrum to convey the deception** to adversary intelligence or tactical sensors. Forces assigned to the

deception effort are often **electronically “enhanced”** to project a larger or different force structure to adversary sensors. Friendly EA assets may be an integral part of the deception effort by **selectively jamming, interfering, or masking** the EM profile of the main operational effort. At the same time, coordination within the JTF staff must occur so that EA activities do not interfere with frequencies being used to convey the EM aspects of the deception to adversary sensors. Disciplined EMCON and other appropriate EP efforts, by both deception assets and those of the main effort, are essential to preventing the adversary from distinguishing deception activities from the main effort. ES assets can **provide immediate warning to deception forces** about adversary forces reacting to their presence or actions. ES assets are also an important means to determine that the adversary is capable of receiving the EM aspects of a deception. Since deception forces are often positioned “off axis” from the main effort, ES platforms positioned with the deception effort may assist in **location of adversary forces** by assisting with “triangulation” in direction finding activities. Designated EW staff personnel should have the security clearances and access necessary to work with military deception planners during the planning and execution phases of an operation which involves deception. EW planners should ensure that EM frequencies necessary in order to support deception plans are accounted for in spectrum management databases and on the JRFL without disclosing that specific frequencies are related to deception. During the execution of an operation, EW staff personnel should **monitor EW support to the deception effort** and coordinate any changes or conflicts in a timely manner.

JP 3-58, “Joint Doctrine for Military Deception,” provides additional details.

- **Physical Destruction.** “**Precision strike**” is an increasingly important aspect of physical destruction actions in joint operations. EW is an important part of precision strike. **Frequency management and deconfliction** must account for frequencies used by various types of precision strike weapons. ES assets are an important part of efforts to dynamically map the EME of the operational area for targeting and threat avoidance planning. Stand-off munitions and anti-radiation ordnance are major assets in any operation and may, for example, be used to selectively destroy adversary emitters in support of military deception, SEAD, OPSEC, and PSYOP efforts. The employment of anti-radiation weapons must be de-conflicted with

friendly and neutral emitters to ensure that engagements between friendly forces are prevented. **Destructive DE weapons** are becoming an increasingly important part of the physical destruction actions of joint operations. EA assets perform vital screening functions (including the use of standoff weapons) for friendly air strikes and other combat units on the ground and at sea. EA also plays an important role in **defeating hostile air strikes and countering precision strike weapons**. Disciplined EMCON and other EP measures are also an important part of protecting friendly air strikes and front line tactical units on the ground and at sea. EMCON and other EP measures also **protect friendly forces handling or operating** around live ordnance during combat operations by preventing inadvertent detonations due to HERO. ES assets **provide timely warning of**

INTEGRATION OF ELECTRONIC WARFARE, DECEPTION, AND PHYSICAL DESTRUCTION IN SUPPORT OF OPERATION OVERLORD

By the evening of June 5, when the vanguard of the invasion fleet set out from England, all but sixteen of the original ninety-two radar sites along the northern coasts of France and Belgium had been attacked from the air. Most of their sets were now out of action, including all of the long range early warning Wassermann and Mammut radars. Now that the “softening up” phase of OVERLORD was complete, the jamming and spoofing phases could go ahead.

On the night of June 5, the two ghost invasion armadas “set sail.” The larger, with Rope dropped from eight Lancaster bombers of No. 617 Squadron of the RAF (the Dam Busters), made for Le Havre - this was Operation TAXABLE. The smaller, flown by six Stirlings of No. 218 Squadron, made for the Dunkirk, Calais and Boulogne area - this was Operation GLIMMER. Orbiting to the north of the real and ghost invasion fleets were four B-17s of the US 803rd Bombardment Squadron (on their first operational mission) and sixteen Stirlings of the RAF No. 199 Squadron. These aircraft put up a Mandrel screen to cover the various operations with the jamming deliberately thin to the east to allow the German operators to observe the TAXABLE and GLIMMER spoofs.

Beneath the orbiting aircraft and their falling clouds of Rope, the small flotilla of launches headed south into the choppy sea with their ungainly “Filbert” balloons trailing low over the water downwind.

SOURCE: Alfred Price
The History of U.S. Electronic Warfare. Volume I, 1989

adversary reaction to friendly air strike and other physical destruction actions that take friendly forces into hostile territory or contact with adversary combat forces. ES also performs an important combat assessment role by providing **feedback about the results of friendly physical destruction actions** that can be obtained through SIGINT or changes in the EME. ES can also be used to evaluate the effectiveness of friendly force EMCON measures and recommend modifications or improvements. All of these factors require that joint EW staff personnel actively work with air planners, fire support personnel, and other staff personnel involved in coordinating the physical destruction actions during combat operations.

JP 3-09, "Doctrine for Joint Fire Support," provides further details.

- **Computer Network Attack and Computer Network Defense.** CNA and CND operations target and defend computer networks and systems. As many computer networks are linked electronically, incorporating the results of EW planning is crucial to both offensive and defensive computer network warfare operations. While physical access to a particular computer network may be limited, electronic access may prove the key to successful computer system penetrations.
- **Legal.** Legal review is required to ensure LOAC compliance.

See JP 1-04, "Joint Tactics, Techniques, and Procedures for Legal Support to Military Operations," for further details.

d. **Exploitation of Captured Equipment and Personnel.** Exploitation of adversary

equipment can verify adversary electronic equipment capabilities, to include WARM. This information can lead to the testing or verification of friendly EW equipment or begin the process of EW reprogramming to counter new adversary capabilities. Exploitation of captured adversary personnel can lead to discoveries of adversary capabilities, tactics, and procedures against friendly EW capabilities. Interrogation of captured personnel may help EW planners **evaluate the effectiveness of friendly EW actions**. This information can also aid in **after-action report reconstruction** of EW. The joint captured materiel exploitation center and joint interrogation and debriefing center conduct theater exploitation of captured material and interrogation of captured personnel respectively. The EW staff should establish EW exploitation and interrogation requirements through the J-2 representative of the IO cell (or via other established procedures) to take advantage of the opportunities that may be realized through the exploitation of captured equipment and the interrogation of captured personnel.

3. **EW Frequency Deconfliction**

The following items are critical elements in the EW frequency deconfliction process and should be performed on a continuing basis (see Figure IV-3).

- a. **Conflict.** EW planners should be prepared to examine cases where **EA missions conflict with the JRFL** or where **JRFL changes might affect planned EA operations**. The extent of conflict analysis depends on the tools and time available to the EW staff. Joint EW personnel should attempt to resolve or diffuse the conflict by working within the staff and subordinate EW units. If the deconfliction effort is successful, the operation is conducted as planned or modified. For unresolved conflicts, J-3 remains the ultimate authority on EW frequency deconfliction.

CRITICAL ELEMENTS IN THE ELECTRONIC WARFARE FREQUENCY DECONFLICTION PROCESS



CONFLICT: Electronic warfare planners should be prepared to examine cases where electronic attack (EA) missions conflict with the joint restricted frequency list (JRFL) or where JRFL changes might affect planned EA operations.



JAMMING: The J-3 decides whether the jamming mission is necessary for success of the operations. If the overall joint force operation can be executed without the jamming mission, the J-3 should probably cancel the jamming mission.



DISRUPTION: When the operation is successful and the friendly EA missions do not disrupt friendly communications networks or non-communications equipment operations, no frequency conflict occurs. However, when any disruption on a friendly frequency occurs, two actions should take place: a report of the disruption should be made as soon as possible to the J-6 spectrum manager and, if critical functions are interfered with, a *CEASE BUZZER* notification should be issued.



RESOLVING INTERFERENCE: If the spectrum manager can determine that the disruption was caused by friendly EA, then the report should be given to the information operations cell for resolution and possible modification of the JRFL.

Figure IV-3. Critical Elements in the Electronic Warfare Frequency Deconfliction Process

b. **Jamming.** In joint operations, **jamming is a form of nonlethal fires** as discussed in JP 3-09, “Doctrine for Joint Fire Support.” As nonlethal fire, the determination to conduct jamming is made in accordance with the principles set forth in Chapter III of JP 3-09. Joint EW planners should be familiar with the process and principles of joint fire support and provide appropriate guidance and coordination necessary to deconflict jamming with other friendly uses of the EM spectrum. Close, continuous coordination with component planners and with allied and coalition planners (during both the planning and execution phase of joint operations) is necessary to ensure that the jamming missions are **conducted as planned and necessary while minimizing unintended disruption of**

the EM spectrum. OPLANs should include provisions for an on-station JCA who will provide real-time coordination and deconfliction of jamming efforts. The JCA does not need to be an EA asset, but should be capable of monitoring the ES spectrum, assessing effects on both friendly and unfriendly forces, and be in contact with EA assets to provide direction and coordination of EA efforts.

c. **Disruption.** When the operation is successful and the friendly EA missions do not disrupt friendly communications networks or non-communications equipment operations, no frequency conflict occurs. However, when any disruption on a friendly frequency occurs, two actions should take

ELECTRONIC DECEPTION IN WORLD WAR II

During May 1944, Cockburn ran a ghost “fleet” toward captured German Seetakt, Freya, and Wuerzburg radars set up on cliffs overlooking the Firth of Forth in Scotland. The spoof worked effectively against all of them. The Allied radar operators, however, had all known they were seeing a simulated invasion fleet. The next stage was to test the spoof against operators who had not been told what to expect. Eight bombers flew a ghost “fleet” against a British Type 11 radar, the nearest equivalent to the Giant Wuerzburg, situated at Flamborough Head on the Yorkshire coast. The unsuspecting operators reported the echoes on their screens as coming from a very large convoy indeed - far larger than any they had seen before. Now Cockburn and his team could be reasonably confident that the spoof would also work against German operators.

SOURCE: Alfred Price
The History of U.S. Electronic Warfare, Volume I, 1989

place: a **report of the disruption should be made** as soon as possible to the J-6 spectrum manager and, if critical functions are interfered with, the **controlling authority for CEASE BUZZER** (an unclassified term used to terminate EA activities, including the use of EW expendables) **should be contacted** to evaluate the need to issue a CEASE BUZZER notification.

- **Report of Interference.** Report interference using Joint Spectrum Interference Resolution (JSIR) formatted messages in accordance with CJCSI 3320.02, “Joint Spectrum Interference Resolution.” Operators should **report interference through the chain of command** to the J-6 spectrum manager by the fastest means available. As the interference reports are passed through the chain of command, each component with the capability should **attempt to resolve the interference** under its purview. Each component may not have the capability or control over that portion of the spectrum to resolve the conflict, so the report should be forwarded as quickly as possible to a level of command with the capability. Ultimately, all unresolved interference reports reach the J-6, at which time the spectrum manager

should attempt to determine the cause of the interference and resolve the conflict.

- **CEASE BUZZER Notification.** For critical functions (generally those on the TABOO list of the JRFL), an **immediate CEASE BUZZER notification** should be promulgated by the JCA if the interference can be positively identified as friendly EA. The CEASE BUZZER notification is issued for the specific frequency or range only on the EW control net of the offending jammer. No acknowledgment of interference is made on the signal being jammed.

For more information on the JRFL TABOO list, see Appendix B, “Electronic Warfare Frequency Deconfliction Procedures.”

- d. **Resolving Interference.** If the spectrum manager can determine that the disruption was caused by a source other than friendly EA, the J-6 has the option of **modifying the current signal operating instructions or communications plans**. If the spectrum manager determines that the interference was caused by friendly EA, then the report should be given to the IO cell for resolution and possible modification of the JRFL. In either

case, both staffs can report (or have the originating unit report) the suspected interference or jamming to the joint staff through the **JSIR program** for detailed analysis.

4. Component Coordination Procedures

Components requiring EW support from another component should be encouraged to **directly coordinate that support** when possible, informing joint EW planners of the results of such coordination as appropriate. However, at the joint force level, EW planners should be familiar with how this coordination occurs across Service and functional component lines in order to be **prepared to assist and facilitate coordination** when necessary or when requested. An overview of component EW coordination factors and procedures are provided in this section. When the JFC has chosen to conduct operations through functional components, the functional component commanders will determine how their components are organized and what procedures are used. EW planners should coordinate with the functional components to determine how they are organized and what procedures are being used by functional component forces.

a. **Army Coordination Procedures.** The Army component headquarters supporting the joint force is responsible for **Army coordination of joint EW support**. Within this headquarters (which may be a theater army, Army group, field army, or corps), requirements for other component EW support are **established by the EW officer in coordination with the G-3** and, if at corps level, in coordination with both the G-3, the fire support coordination center or fire support element (FSE), and the G-6. These requirements are translated into EW support requests and, where possible, are coordinated directly with the appropriate staff elements

having EW staff responsibility within other component headquarters. Conversely, other components requiring Army EW support initially coordinate those support requirements with the EW officer at the Army forces headquarters or tactical operations center. This coordination is normally done in person or through operational channels in planning joint EW operations. However, the Global Command and Control System (GCCS) or Army Global Command and Control System (AGCCS) may be used to **coordinate immediate requests for Army EW support**. In this case, other components will communicate their EW support requests via the GCCS or AGCCS to the FSE and EW officer or to the EW section at corps or division level. Air Force and Army coordination will normally **flow through the battlefield coordination detachment** at the Air Force Air Operations Center. EW staffs at higher echelons monitor the EW requests and resolve conflicts when necessary. Also, the G-3:

- Provides an assessment of EW capabilities to other component operation centers;
- Coordinates preplanned EW operations with other Service components; and
- Updates preplanned EW operations in coordination with other components as required.

b. **Marine Corps Coordination Procedures.** The MAGTF headquarters **EWCC**, if established, or the MAGTF **EW**O, if there is no EWCC, is responsible for **coordination of the joint aspects of MAGTF EW requirements**. Requirements for other component EW support are established by the operations staff, in coordination with the aviation combat element, the ground combat element, and the combat service support element of the

MAGTF. These requirements are translated by the EWCC or EWO into tasks and coordinated with the other component EW staffs. In addition, the EWCC or EWO:

- Provides an assessment of Marine Corps forces' EW capabilities to other component operation centers to be used in planning MAGTF EW support to air, ground, and naval operations;
- Coordinates preplanned EW operations with appropriate component operation centers;
- Updates EW operations based on coordination with other component EW agencies; and
- Coordinates with the intelligence staff officer to ensure that an intelligence gain and loss analysis is conducted for potential EW targets.

c. **Navy Coordination Procedures.** In naval task forces, the **IWC is normally collocated with the CWC** and is directly responsible for all aspects of EW, including necessary joint coordination. When naval task forces are operating as a component of a joint force, the IWC:

- Provides an assessment of Navy EW capabilities to the other component operation centers; and
- Coordinates preplanned EW operations with appropriate component EW agencies.

NOTE: Airborne EA and ES assets, such as the EA-6B Prowler, when employed in a strike support role will be the responsibility of the strike warfare commander. The strike warfare commander is the CVWC or the more traditional CAG. The CAG is responsible for

coordinating integration of air wing assets into the ATO with the JFACC.

d. **Air Force Coordination Procedures.**

Air Force requirements for other component EW support are established by the **COMAFFOR's A-3 or A-5**, in coordination with the Director for Intelligence. The A-3 or A-5 staff translates requirements for other component EW support into tasks and coordinates those tasks with the component EW agency. In addition, the A-3 or A-5 staff officer:

- Provides an assessment of Air Force capabilities to other component operation centers; and
- Updates EW operations based on coordination with the other component agencies.

e. **Special Operations Forces Coordination Procedures.** The joint force special operations component command (JFSOCC) will establish a **JOC** to serve as the task integration and planning center for joint force special operations (SO). Requirements from SO units for EW support will be transmitted to the JFSOCC JOC for coordination with the JFSOCC IO cell.

See JP 3-05, "Doctrine for Joint Special Operations," for further details.

f. **United States Coast Guard (USCG).**

In peacetime the USCG operates as part of the Department of Transportation. In wartime the USCG will operate as part of the Department of Defense. During both peacetime and war, joint operations may include USCG assets that may possess EW capabilities. Coordination with USCG assets should be through assigned USCG liaison personnel or operational procedures specified in the OPLAN or OPORD.

5. EW and Intelligence Coordination

Detailed coordination is essential between the EW activities and the intelligence activities supporting an operation. A major portion of the intelligence effort, prior to and during an operation, relies on collection activities that are targeted against EM energy in various parts of the EM spectrum. ES depends on the **timely collection, processing, and reporting of various intelligence** to alert EW operators and other military activities about important intelligence collected in the EM spectrum. It is vital that all prudent

measures are taken to **ensure that EA activities and other friendly EW activities are closely and continuously deconflicted with ES** and other intelligence collection activities. The J-2 must ensure that EW collection priorities and ES sensors are integrated into a **complete intelligence collection plan**. This plan ensures that scarce intelligence and ES collection assets are maximized in order to support all aspects of the JFC objectives.

JP 2-01, “Joint Intelligence Support to Military Operations,” and its classified supplement provide additional details.

CHAPTER V

ELECTRONIC WARFARE IN JOINT EXERCISES

"We must remember that one man is much the same as another, and that he is best who is trained in the severest school."

Thucydides

1. Introduction

Effective employment of EW in joint operations depends on the ability of US forces to train as they intend to fight. Joint exercises are a unique opportunity to **exercise component EW capabilities in mutually supportive operations**. Because of the complexity of good EW planning and the impact that EW has on many other areas of joint operations, EW should be included in most joint exercises. The potential for EW (particularly EA actions) to disrupt the use of the EM spectrum and thereby disrupt other training objectives of an exercise require that **EW exercise activities be well planned in order to balance EW training objectives with other training objectives**.

2. Planning Joint Exercises

Exercise planning is a separate process from the JOPES planning, which is used to develop OPLANs. While the development of an OPLAN using the JOPES planning process is usually part of the training that takes place during joint exercises, exercise planning involves all the **necessary preparations to structure the exercise and facilitate training**. Most joint exercises are scheduled at an **annual exercise planning conference**. The results of this conference are promulgated in Chairman of the Joint Chiefs of Staff (CJCS) Notices. CJCS Notice 3501, "CJCS Joint Training Master Schedule," is a long-range planning document that provides nominal exercise schedules for 5 fiscal years. More detailed scheduling guidance is provided in CJCS Notice 3502, "Quarterly Schedule of Significant Military Exercises."

These two documents identify the scheduling command, sponsoring command, and the name, dates, location, and purpose of the exercise as well as joint tasks (from CJCSM 3500.04B, "Universal Joint Task List") to be trained during the exercise. More information about the joint training program can be obtained from CJCSM 3500.03, "Joint Training Manual for the Armed Forces of the United States." Planning for joint exercises normally occurs several months prior to start of the exercise (STARTEX). **The planning process is anchored by three planning conferences** hosted by the sponsoring command: the **initial planning conference** (IPC), the **mid-planning conference** (MPC), and the **final planning conference** (FPC). The tasks that must be accomplished by EW planners during this planning period are addressed in the following section.

3. Planning EW in Joint Exercises

a. The exercise-sponsoring command normally designates those commands or staff personnel responsible for planning the specific aspects of the exercise. The command or person designated to plan the EW aspects of an exercise must be concerned with:

- **Identifying EW exercise objectives** that are consistent with the overall exercise objectives in scope, purpose, and level of effort;
- **Developing an EW concept of operations** (for "Blue" and "Red" forces) that is integrated into the larger concept of operations;

- **Coordinating EW personnel and assets** to participate as both “Blue” and “Red” forces (if specific force participation has not already been designated by higher authority);
- **Identifying personnel with EW expertise** to participate as joint exercise control group (JECG) and “White cell” participants;
- **Determining EW modeling and simulation requirements and systems** for the exercise and coordinating their availability and funding; and
- **Drafting the EW sections of the exercise directive** and supporting plans such as the exercise control plan. Figure V-1 gives a general idea of the planning flow involved in planning EW in exercises.

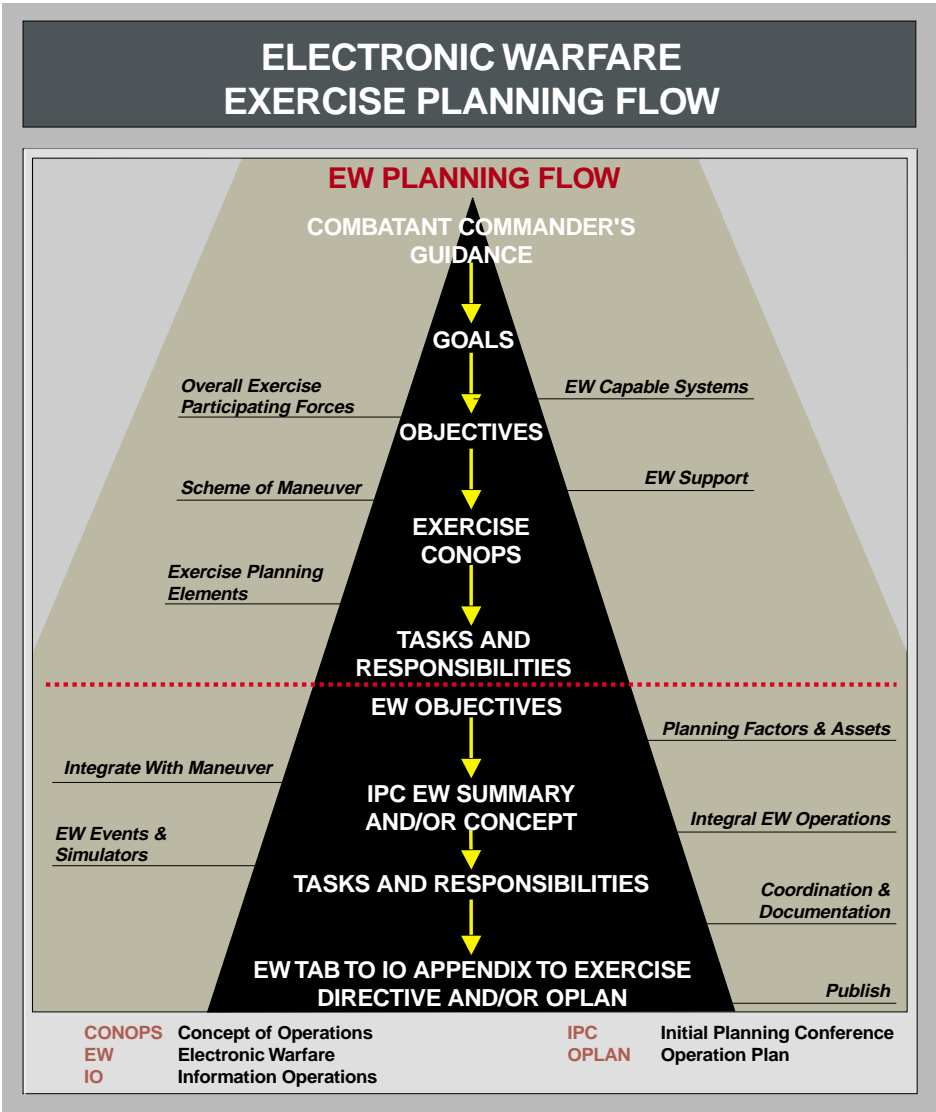


Figure V-1. Electronic Warfare Exercise Planning Flow

b. Planning Considerations. When employing EW in exercises, fundamental planning considerations include the following.

- The exercise objectives and how they relate to EW. Planning EW exercise objectives should include a review of the universal joint task list, the Joint Mission Essential Task List, and the Chairman's Commended Training Issues for applicable objectives.
- The type of exercise, the location and size of the exercise area, and the duration of the exercise.
- Lessons learned from previous, similar joint exercises and operations. The review of lessons learned is an important and cost effective way to avoid the documented mistakes of previous exercises and operations.
- The number and type of EW assets and personnel that will be appropriate for the type of exercise and its objectives.
- The type of control (free play, semi-controlled, controlled, or scripted) for EW activities that will be necessary to most effectively accomplish the training objectives.
- The type of modeling or simulation system that will be used as part of the exercise.
- The number of EW experienced evaluators that will be necessary to adequately monitor the exercise and assist in developing lessons learned through the after-action report (AAR) process.
- **Evaluate the potential for interference between EW and EM activity (civilian and military) outside the scope of the exercise.** Avoiding exercise conflicts

with third party EM spectrum use involves adherence to guidance provided in training area standing operating procedures (SOPs) as well as applicable local regulations, laws, treaties, and conventions. For exercises conducted in the United States or Canada, EW exercise planners must consult CJCSM 3212.02, "Performing Electronic Attack in the United States and Canada," for planning guidance and procedures. The JSC can assist in accomplishing this task. However, EW planners should coordinate with J-6 and request assistance from the JSC early in the planning process.

- **Evaluate the possible adverse effect of compromising friendly operations, intelligence capabilities, and methods.** "Real-world" OPSEC and other security considerations must be taken into account when planning EW activities. Foreign intelligence organizations often monitor joint exercises to gather information about US capabilities, tactics, and procedures.

c. Planning Tasks. The following tasks (shown in Figure V-2) should be undertaken to ensure that EW is properly integrated into joint exercises when appropriate.

- **Development of specific, attainable EW exercise objectives.** EW exercise objectives are statements of anticipated effects that result from specific EW actions. The identification and accomplishment of these objectives will increase the capability of effectively employing the EW resources and provide the vehicle to evaluate the training of EW personnel. **Objectives must be measurable and compatible with overall exercise constraints.** EW objectives should provide specific direction and should be correlated, when possible, to lessons learned or the

TASKS TO INTEGRATE ELECTRONIC WARFARE INTO JOINT EXERCISES

Develop specific, attainable electronic warfare (EW) exercise objectives.

Provide the opportunity for sufficient EW activity to accomplish exercise objectives and satisfy training requirements.

Create as realistic an exercise environment as possible.

Encourage commanders to practice EW frequency deconfliction procedures during exercises.

Ensure adequate manning for EW staff functions and EW evaluations.

Ensure that "real-world" operations security is considered in the exercise planning effort.

Coordinate the use of simulations to fulfill training objectives.

Figure V-2. Tasks to Integrate Electronic Warfare Into Joint Exercises

development of new tactics, techniques, and procedures. General statements of policy and rephrased definitions should be avoided in the development of objectives.

- **Provision of the opportunity for sufficient EW activity to accomplish exercise objectives and satisfy training requirements.** The quantity and type of EW activity appropriate to each joint exercise are related to the **type of exercise, the overall exercise training objectives, and the type and quantity of EW assets and personnel** involved.

EW exercise planners should consider these factors when proposing EW events and drafting the EW portion of the exercise directive. EW activities within an exercise can be stimulated through **scenario design and asset participation** or through **scripting of specific events** in the master scenario events list (MSEL). In addition to the training value of coordinating and employing multiple Service EW platforms in a joint environment, joint exercises offer the opportunity for EW personnel to exercise staff EW functions such as the EW reprogramming process.

EW exercise planners should review the principal EW techniques discussed in Chapter I, “Overview of Electronic Warfare,” for ideas about the type of EW exercise activities that may be scheduled to achieve training objectives.

- **Creation of as realistic an exercise environment as possible.** For training purposes the EW environment in an exercise should be as realistic as possible. However, the need for realism to support training must be weighed against the **concern for safety and avoiding disruption of the EM spectrum** used by third parties. As past exercise experience has shown, even seemingly harmless activities such as releasing chaff in offshore operations areas can have unintended consequences if the chaff is blown ashore and shorts out high power lines. Realism can be achieved by **using friendly EW assets or by employing EW models and simulations**. To achieve exercise objectives, it is often necessary to employ available EW assets alternately in “Blue” and “Red” roles.
- **Practice of EW frequency deconfliction procedures** as discussed in Chapter IV, “Coordinating Joint Electronic Warfare,” and Appendix B, “Electronic Warfare Frequency Deconfliction Procedures,” during exercises. Frequency deconfliction is an important part of joint operations, and practicing these procedures routinely during exercises should be an important training goal for commanders in order to **prepare for most real-world operations**.
- **Provision for adequate manning for EW staff functions and EW evaluations.** EW planners should nominate EW manning billets through the process being used to create the

exercise billet documents. In addition to the appropriate number of EW billets in the exercise joint staff, EW observer and training billets and EW “white cell” billets may be appropriate, depending on the scale and purpose of the exercise. If EW-related technology or tactics evaluations are to be accomplished during the exercise, additional EW evaluation billets may be necessary.

For more information on EW billets in the exercise joint staff, see the EW manning section of Chapter II, “Organizing for Joint Electronic Warfare.”

- **Provision to ensure that “real-world” OPSEC is considered in the exercise planning effort.** Coordinate with appropriate authorities to ensure that **adequate protection is applied for both simulators and real-world systems**. These systems should be used at locations and in ways that minimize the success of collection efforts of hostile intelligence systems.
- **Coordination of the use of simulations to fulfill training objectives.** Force-on-force simulations provide a capability to **train battle staffs in the planning, execution, and evaluation** of EW employment for any range of scenarios, from a small single-Service counterdrug exercise to a multinational theater campaign. A current EW model used by the Warrior Preparation Center and the Battle Training School is the Joint Electronic Combat Electronic Warfare Simulation, which is linked to the Air Force Air Warfare Simulation System model.

Appendix E, “Electronic Warfare Modeling,” provides additional details about EW modeling and simulation.

d. **EW Exercise Planning Flow.** The planning tasks discussed in the previous paragraph must be accomplished within the framework of the **three phases of exercise planning**, culminating in the **IPC, MPC, and FPC**, respectively. Normally, the IPC occurs approximately 8 months prior to the commencement of the exercise. The MPC follows the IPC by about 4 months. The FPC normally occurs about 2 months before the exercise. EW exercise planning tasks normally should be accomplished within this framework as discussed below.

- **Initial Planning Tasks.** The initial planning phase of each exercise normally begins with the issuance of the sponsoring command's guidance concerning the exercise. The development of an outlined **EW concept of operation** and the drafting of **specific EW training objectives** are primary planning functions that should be accomplished during this phase. Key Service, support agency, and multinational participants should be contacted to determine their proposed level of participation and any objectives or constraints that they may recommend for planning consideration. **Early coordination with exercise IO planners** is also important to ensure that the EW concept of operations and EW training objectives support and are supported by the broader IO concept and objectives. An **initial assessment** should be made of possible **conflicting demands on EW assets** within the exercise, between the exercise being planned and other joint or Service exercises, and between exercise and real-world operations. **EM spectrum management procedures, constraints, and regulations** specific to the exercise area should be identified during this phase of planning. Service, supporting agencies, and appropriate multinational participants should be

invited to participate in the IPC. The EW focus at the IPC should be on meeting key participants, reviewing the basic EW concept of operations and EW training objectives, and proposing how to work through any asset scheduling conflicts or issues of concern. Any special maintenance or support requirements unique to EW assets to be used in the exercise, along with the movement of EW assets and personnel to and from the exercise area, are topics which may prove useful for discussion among participants during the IPC.

- **Mid-Planning Tasks.** The period between the end of the IPC and the MPC is the time when **the EW concept of operation, training objectives, and other planning tasks should be finalized**. After finalization, all changes and updates concluded during the MPC will have a due date of the FPC. An EA on-off control plan should be developed during this phase to **ensure the priority of safety** for any active jamming or other measures anticipated during the exercise. Frequency assignments are made during this phase and frequency plans are promulgated. EW exercise planners should coordinate with IO exercise planners and J-6 exercise planners to coordinate the assignment of frequencies (for "Blue," "Red" and JECG) necessary to accomplish EW training objectives. The **exercise directive is normally finalized during this phase**, and EW planners should **accomplish planning tasks** to complete the EW portion of the exercise directive in order to conform to the timeline for promulgation of this and supporting documents. Timely distribution of the exercise directive and support documentation is necessary in order to give exercise participants time to complete preparations and conduct any pre-exercise training that may be necessary.

- **Final Planning Tasks.** The final aspects of EW planning for an exercise, as well as the FPC, are actually accomplished in the preparation stage of the exercise and are discussed in paragraph 4.a. below.

4. EW in Exercise Preparation, Execution, and Post-Exercise Evaluation

The planning stage is only the first of four stages in the life cycle of each joint exercise (see Figure V-3). The other three stages, **preparation, execution, and post-exercise and evaluation**, also involve tasks and coordination on the part of EW exercise staff personnel.

a. **Preparation Stage.** During the preparation stage, the approved **exercise**

directive and supporting plans are distributed; pre-exercise training is developed and conducted; any exercise specific **databases are finalized and tested;** and the **exercise time-phased force and deployment data is validated.** During this stage, milestones receive a final review and update, operation plans and orders are finalized, simulation gamer augmentees and AAR observer manning is completed, and the AAR collection management plan is approved. The **FPC is conducted** in order to finalize actions required prior to STARTEX. Key action of the FPC includes time-phased force and deployment list refinement as well as the concept of operations and MSEL review as applicable. EW preparations during this period include obtaining necessary clearances and notifications for EW activity (particularly EA), coordinating implementation of the

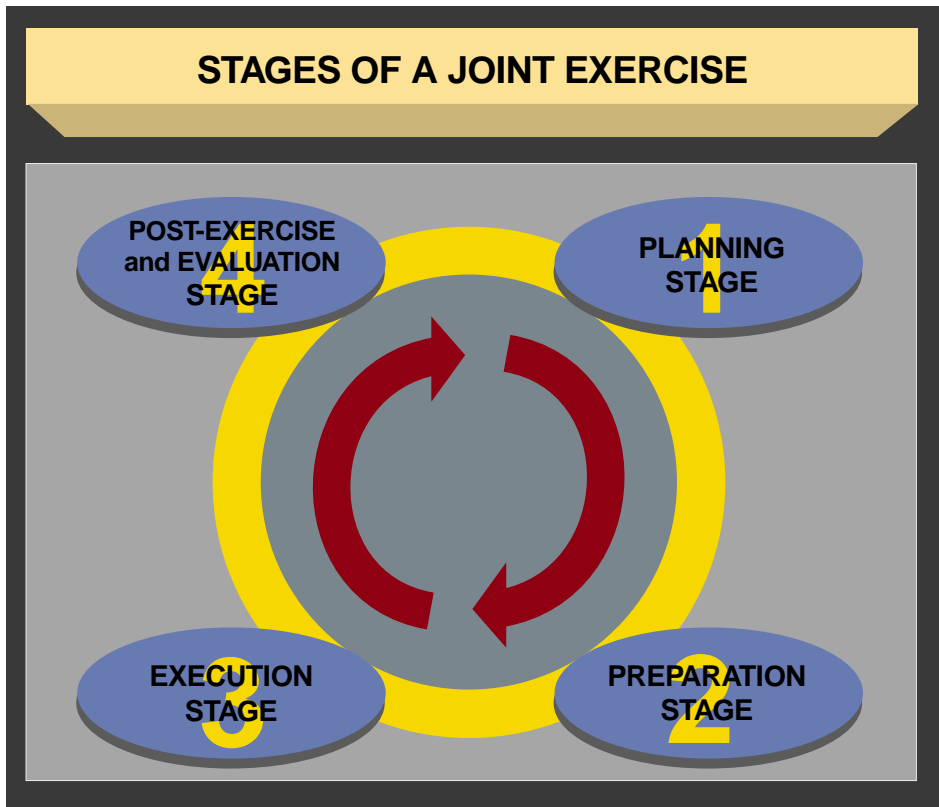


Figure V-3. Stages of a Joint Exercise

exercise directive, and accommodating changes in personnel and assets.

b. **Execution Stage.** During the actual conduct of the exercise, personnel responsible for the EW aspects of the exercise should focus their efforts on ensuring that the **EW events in the MSEL occur as planned**, that actual EW exercise activities remain **focused on the training objectives**, and that **data and observations** that support the AAR process are properly **collected and processed**. Prior to the actual STARTEX, it may be necessary or useful to provide structured training on some aspect of EW as a means to achieve one or more of the training objectives. The

specifics of such training (who will instruct, who will attend, where, and other specifics) should be worked out during the planning and preparation stages of the exercise.

c. **Post-Exercise and Evaluation Stage.** This period actually **begins prior to the conclusion of the exercise**. EW activity associated with this stage includes capturing and documenting lessons learned, participating in “hot wash” meetings, and coordinating the redeployment of participants and assets to parent commands.

The form and format for documenting lessons learned is in CJCSI 3150.25, “Joint After-Action Reporting System.”

CHAPTER VI

MULTINATIONAL ASPECTS OF ELECTRONIC WARFARE

"Durable relationships with allies and friendly nations are vital to our security. A central thrust of our strategy is to strengthen and adapt the security relationships we have with key nations around the world and create new relationships and structures when necessary."

National Security Strategy for a New Century

1. Introduction

Operations DESERT STORM and ALLIED FORCE demonstrated the requirement for US forces to be able to integrate operations with other allied and coalition nations. US planners must be prepared to integrate US and allied or coalition EW capabilities into an overall EW plan, be able to provide allied or coalition nations with information concerning US EW capabilities, and provide EW support to allied or coalition nations. As in joint operations, **EW is an integral part of multinational operations.** In US-led operations, the doctrine within this publication should be used as the basis for all EW activities within the Multinational Force (MNF). However, the planning of MNF EW is made more difficult because of **ill-defined security issues, different crypto equipment, differences in the level of training** of involved forces, and **language barriers.** These problems are well understood throughout North Atlantic Treaty Organization (NATO) commands and are normally resolved by **adherence to agreed-upon procedures.** Therefore, it makes sense for US forces, as participants in NATO, to adopt these procedures when working with NATO or other MNFs such as may be drawn from members of the American, British, Canadian, Australian Armies Standardization Program (ABCA) and the Air Standardization Coordinating Committee (ASCC) made up of the members of ABCA plus New Zealand. NATO and the ABCA have developed documents to deal with MNF EW mission support, and are currently developing a

doctrine for multinational operations. ASCC is developing a document to cover MNF EW support and operations that will draw from this publication. As a result of these publications, most allied and coalition EW officers can be expected to understand the subject. However, with the exception of Australia, Britain, and Canada (who are on the official distribution list of this publication), allied and coalition EW officers may not understand the terminology or procedures being used. A fundamental task for the EWO of a US-led MNF is to **recognize and resolve terminology and procedural issues** at the outset. This can be achieved by comparing multinational doctrine to this publication. **Current NATO EW doctrine is largely based on US EW doctrine.** Geographic combatant commanders should provide guidance to the MNF commander (MNFC) (if the MNFC is a US Service member) within their joint OPLANs on the release of classified material to allied and/or coalition forces. However, the MNFC must determine the need to know and release information essential to accomplishing the mission at the earliest stages of planning. To do this, US EW planners must be intimately aware of both sides of the issue — national security as well as mission accomplishment — in order to advise the MNFC.

2. MNF EW Organization and Command and Control

a. **MNFC.** The MNFC **provides guidance for planning and conducting EW operations to the MNF** through the J-3 and

the IO cell. It should be recognized that the IO cell (or EW planning cell if implemented), for all intents and purposes assumes responsibilities set forth in Chapter II, “Organizing for Joint Electronic Warfare.”

b. **Multinational Staff.** The MNFC should assign responsibilities for management of EW resources in multinational operations among the staff as follows.

- **Operations Officer.** The multinational staff J-3 has primary responsibility for the planning and integration of EW operations with other combat disciplines.
- **Staff EW Officer.** The staff EWO’s primary responsibility should be to ensure that the MNFC is provided the same EW support that a US JFC would expect. In addition to the duties outlined in Chapter II, “Organizing for Joint Electronic Warfare,” the EW officer should be responsible as follows.

- Ensure that all component commanders of the MNF **provide adequately trained EW officers** to be members of the MNFC EW staff. The chain of command should be established by the J-3. The rationale for augmentee status is that the allied and/or coalition officers must be full members of the multinational EW planning cell and responsible to the chain of command. They must not be subjected to the possibility of split loyalties to a lower command within the force, as could be the case if they adopted the traditional liaison role.

- Determine the need for placing US EW liaison officers with allied and/or coalition commands to ensure that the MNFC’s EW **plans and procedures are correctly interpreted.**

- **Integrate allied and/or coalition EW officer augmentees** at the planning stage, delegating to them duties and responsibilities similar to those given to equivalent US officers.

- **Coordinate the necessary EW communications connectivity** for assigned forces. Particular emphasis should be given to equipment, encryption devices and keying material, and procedural compatibility when integrating allied and/or coalition forces.

- Integrate allied and/or coalition C2 requirements into the multinational and joint restricted frequency list.

- At the earliest possible stage, provide allied and/or coalition forces with current US EW doctrine and planning guidelines.

- **Allied and/or Coalition EW Officers.** Allied and/or coalition commanders should assign adequately trained EW officers to the MNF EW planning cell. These officers should:

- Have an in-depth knowledge of their own forces’ operational requirements and capabilities, organize SIGINT and EW capabilities, national support facilities, and C2 structure; and

- Possess national clearances equivalent with the level of classified US military information they are eligible to receive in accordance with US national disclosure policy. These requirements may mean the individuals concerned will be a senior O-3 or O-4 paygrade level or equivalent. As a result, they may be augmentees drawn from national sources other than the unit involved in the MNF.

3. Multinational EWCC with NATO Forces

Although NATO's EW doctrine, contained in Military Committee (MC) document 64, "NATO Electronic Warfare Policy," is largely based on US EW doctrine, the **perspective and procedures of an MNF EWCC will be new to most**. At best, participants may have worked joint issues and served in adjacent forces who have exchanged EW liaison officers. However, precedent exists; maritime forces have for many years worked multinational issues with little difficulty. Allied Tactical Pub (ATP) 8A, "Doctrine for Amphibious Operations," now contains a supplement on EW. This includes procedures necessary to exchange SIGINT information. In addition, NATO is developing Allied Joint Pub (AJP)-01(A), "Allied Joint Operations Doctrine," which will include a chapter on EW and the EWCC. ATP-44, "Electronic Warfare in Air Operations," and ATP-51, "Electronic Warfare in the Land Battle," are additional NATO EW publications available to multinational forces. NATO members invariably base their national EW doctrine on that agreed within NATO MC 64. However, there is a need to ensure that the most recent, releasable, US EW publications are provided to supporting allied and/or coalition forces. NATO has also established a NATO emitter database to exchange information about member countries' electronic emissions and facilitate the coordination of EW.

4. Multinational EW with ABCA and ASCC Member Nations

Strong ties are maintained with these traditional allied forces. This is particularly true within the field of EW and SIGINT. **Much information is exchanged at the national level** and this publication has been released to these nations. An example of the close ties is the Quadripartite Working Group

on EW, which is the ABCA EW forum. Although Australia is not a party to NATO agreements, they are aware of the current status of NATO's EW doctrine contained in MC 64. Quadripartite Standardization Agreement (QSTAG) 593, "Doctrine on Mutual Support Between EW Units," reflects current NATO doctrine and meets Australia's needs. This document contains SOP for an EWCC. ASCC Working Parties (WPs) 45 (Air Operations) and 70 (Mission Avionics) both deal with EW issues. WP 45 looks at the operational employment of the MNF's EW assets, while WP 70 investigates the possibility of standardizing EW systems.

5. Multinational EWCC with Non-NATO or ABCA Allies or Coalition Partners

The principles expressed above are equally applicable to other allies and/or coalitions. The MNFC should include EW officers from supporting allied and/or coalition forces within the EWCC. Should this not be practical for security reasons or availability, the MNFC should, based on the mission, be prepared to provide EW support and the appropriate liaison officers to the allied and/or coalition units.

6. EW Mutual Support

a. **Exchange of SIGINT information** in support of EW operations should be conducted in accordance with standard NATO, ABCA, and ASCC procedures, as appropriate. The information data elements, identified at TABs 1 and 2 and Annex C, also are contained in appropriate allied publications — notably, NATO's confidential supplement to ATP-8(A), "EW in Amphibious Operations," ATP-51, "EW in the Land Battle," and ABCA's QSTAG 593, "Doctrine on Mutual Support Between EW Units." Care should be taken not to violate SIGINT security rules when exercising EW mutual-support procedures.

b. **Exchange of Electronic Order of Battle.** In peacetime, this type of exchange is normally achieved under **bilateral agreement**. NATO has in place procedures within the Major NATO commanders' precautionary system that can be put into effect during time of tension. They include the requirement to **exchange information on WARM**. The procedures also determine at what stage allied forces change to the use of WARM; however, in low-level conflict, they are unlikely to be activated. Therefore, the EWCC officer, through the EW intelligence support organization and the theater Joint Analysis Center (JAC) or theater JIC, should ensure maintenance of an up-to-date EOB. Allied and/or coalition staff officers should be included in turn, and should ensure that their national commands provide appropriate updates to theater joint analysis in discussions on theater EOB. They, in turn, should ensure that their national commands provide appropriate updates to theater JACs and JICs.

c. **Reprogramming.** Reprogramming of EW equipment is a **national responsibility**. However, the EWCC officer should be aware of reprogramming efforts being conducted within the multinational force. The EWCC officer should keep the MNFC aware of limitations that could result in fratricide and, when necessary, seek the MNFC's assistance in attaining a solution. To do this, national and allied and/or coalition commands should provide the EWCC officer with information on the following on request.

- Capabilities and limitations of MNF allied and/or coalition EW equipment.
- EW reprogramming support available within MNF allied and/or coalition units.
- Bilateral agreements on reprogramming support for allied and/or coalition units employing US EW equipment, to include any agreement on flagging support.

- Bilateral agreements on exchange of EW reprogramming information with those nations not employing US EW equipment.
- Reports from friendly units experiencing reprogramming difficulties, to include information on efforts being made to rectify the problem.
- Immediate reports on incidents that could have resulted in fratricide.
- Operational change requests sent to US foreign military sales reprogramming organizations, that identify deficiencies in the allied and/or coalition country's EW equipment and their request for reprogramming support.

In turn, the EWCC officer should ensure that allied and/or coalition units in the MNF receive the most recent data held within the theater tactical EOB database and, as appropriate, the associated parametric information. This should allow allied and/or coalition units within the MNF to **judge the reliability of their current reprogramming data** and, if necessary, **identify problems** to the MNF EWCC and national support agencies. Without this level of EW mutual support, fratricide may occur.

d. **US EW Planning Aids.** Significant improvements have been made within the United States in the automation of EW planning aids. These improvements allow US EW planners to **extract information**, almost at will, **from theater and national databases and depict it in graphic format** for planning and briefing purposes. Supporting allied and/or coalition forces are unlikely to have an equal level of automation. Working with the allied and/or coalition officers, the EWCC officer should determine what EW information would assist the MNF at the planning and unit level and ensure that they

get it. To do this, the EWCC officer should understand security issues that preclude the release of some of the data and its source but do not necessarily preclude the release of EW mission planning tools.

7. Releasability of EW Information to Allies and Multinational Forces

The integration of allied and/or multinational EW officers into US-led

MNF activities is often perceived by US staff officers as too difficult due to the complexity of national disclosure policy. A clear, easily understood policy on the disclosure of EW information requested by allied and multinational partners must be developed by the commander's IO cell officer. Likewise, in peacetime exercises, the chief IO officer should develop a clear, easily understood policy on the disclosure of EW information.

Intentionally Blank

APPENDIX A

JOPEs ELECTRONIC WARFARE GUIDANCE

The guidance in this annex relates to the development of Tab B (Electronic Warfare) of Appendix 3 (Information Operations) to Annex C (Operations) of the format found in CJCSM 3122.03, “Joint Operation Planning and Execution System Vol II: (Planning Formats and Guidance),” for OPLANs, operation plans in concept format, OPORDs, campaign plans, and functional plans.

1. Situation

a. Enemy Forces

- What are the capabilities, limitations, and vulnerabilities of enemy communications, non-emitting, and EW systems?
- What is the enemy capability to interfere with accomplishment of the EW mission?

b. Friendly Forces

- What friendly EW facilities, resources, and organizations may affect EW planning by subordinate commanders?
- Who are the friendly foreign forces with which subordinate commanders may operate?

c. Civilian and/or Neutral Facilities

- What civilian and/or neutral facilities, resources, and organizations may affect EW planning by subordinates?
- What potential collateral effects could be expected?

d. **Assumptions.** What are the assumptions concerning friendly or enemy

capabilities and COAs that significantly influence the planning of EW operations?

2. Mission

What is the EW mission (who, what, where, why)?

3. Execution

a. Concept of Operations

- What is the role of EW in the commander’s strategy?
- What is the scope of EW operations?
- What methods and resources will be employed? Include organic and non-organic capabilities.
- How will EW support the other elements of IO and SEAD?

b. **Tasks.** What are the individual EW tasks and responsibilities for each component or subdivision of the force? Include all instructions unique to that component or subdivision.

c. Coordinating Instructions

- What instructions, if any, are applicable to two or more components or subdivisions?
- What are the requirements, if any, for the coordination of EW actions between subordinate elements?
- What is the guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered elsewhere in this tab?

- What is the emissions control guidance? Place detailed or lengthy guidance in an exhibit to this tab.
- What coordination with the J-6 is required to accomplish the JRFL?

4. Administration and Logistics

a. Administration

- What, if any, administrative guidance is required?
- What, if any, reports are required? Included example(s).

b. **Logistics.** What, if any, are the special instructions on logistic support for EW operations?

5. Command and Control

a. Feedback

- What is the concept for monitoring the effectiveness of EW operations during execution?
- What are the specific intelligence requirements for feedback?

b. **After-Action Reports.** What are the requirements for after-action reporting?

c. **Signal.** What, if any, are the special or unusual EW-related communications requirements (e.g., PACER WARE and SERENE BYTE)?

APPENDIX B

ELECTRONIC WARFARE FREQUENCY DECONFLICTION PROCEDURES

Annex A Standardized JRFL Format

ELECTRONIC WARFARE FREQUENCY DECONFLICTION PROCEDURES

1. General

Friendly, adversary, and third party operations that use or affect the EM spectrum (communications, non-communications, jamming) have the potential to interfere with joint force communications and other electronic systems. To counter this, the US military has established spectrum management and EW frequency deconfliction procedures. Spectrum management is composed of an entire range of technical and non-technical processes designed to quantify, plan, coordinate, and control the EM spectrum to satisfy spectrum use requirements while minimizing unacceptable interference. EW frequency deconfliction can be considered a subset of spectrum management and is defined as a systematic management procedure to coordinate the use of the EM spectrum for operations, communications, and intelligence functions. This appendix provides guidance for developing joint EW frequency deconfliction procedures. To facilitate the development process, procedures and specific staff responsibilities are discussed in paragraph 5 below. To the extent possible, these procedures should be followed during joint, multinational, and single-Service operations and exercises.

2. EW Deconfliction Procedures

The steps involved in the EW frequency deconfliction process are as follows.

a. Defining the Operations Concept and Critical Functions. The J-3 defines the concept of operations to include each discrete phase of the operation. For each phase, the J-3 defines the critical mission functions that require uninterrupted communications connectivity or non-communications operations. For example, communications

with long-range reconnaissance elements or close air support assets could be crucial to preparing for transition from defense to offense. Non-communications equipment such as identification, friend or foe systems and fire-control radars might also need protection. The J-3 provides this guidance to the joint force staff and subordinate commanders for planning.

b. Developing the Intelligence Assessment. Based on the J-3 concept of operations, the J-2 determines intelligence support requirements and identifies adversary electronic system targets for each phase of the operation (including the critical adversary functions) and associated electronic system nodes that need to be guarded. For example, during the friendly attack, adversary communication and non-communications associated with C2 of the counterattack forces could be crucial to friendly forces in determining the timing of the counterattack and the exact area where the attack will take place. Therefore, those critical nodes should be protected from EA.

c. Managing the Electromagnetic Spectrum. The J-6 is responsible for the administrative and technical management of the EM spectrum. This includes maintaining, in conjunction with the J-2, the necessary database that contains information on all friendly, available adversary, and selected neutral or civil spectrum emitters or receivers. With the aid of the database, the J-6 assigns frequencies, analyzes and evaluates potential conflicts, resolves internal conflicts, recommends alternatives, and participates in spectrum-use conflict resolution. The assignment of frequencies is based on the J-3 concept of operations, frequency availability, unit geographic dispersion, radio wave propagation, equipment technical parameters,

criticality of unit functions. When assigning frequencies, the J-6 should advise users (using their frequency database) of possible interference from mobile systems in the operational area. Operating on assigned frequencies could spell the difference between success and failure of the operations.

d. Defining and Prioritizing Candidate Nodes and Nets. The joint force staff and subordinate commanders should define functions and identify specific nodes, communications and non-communications networks, and equipment that are critical to friendly and adversary operations. Candidate nodes and nets are submitted for EA protection to the EWO in J-3 and/or the IO cell. (The submission should follow the standard JRFL format listed in Annex A, “Standardized JRFL Format.”) In times of tension and war, certain adversary force data derived from compartmented SIGINT information should be provided by the J-2 and may be exchanged at the appropriate level of classification. Real-world EW data elements should not be exchanged in exercises except when specifically authorized.

e. Generating the JRFL. The JRFL is a time- and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. The JRFL should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. Thus, the JRFL facilitates friendly EW actions by placing the minimum number of restrictions on systems such as EC-130H/COMPASS CALL, EA-6B/PROWLER, EH-60/QUICK FIX, and AN/TLQ-17A(V3)/TRAFFICJAM. The J-6 should compile the JRFL based on the coordinated inputs from the operations, intelligence, and communications staffs within the command and affected subordinate commands. The J-6 should ensure that the frequency assignments of unit nets designated for inclusion as PROTECTED or TABOO on the JRFL are submitted to the J-3 for final

approval prior to dissemination. The restrictions imposed by the JRFL may only be removed at the direction of the J-3 if the J-3 determines that the benefit of jamming a restricted frequency surpasses the immediate criticality to friendly forces. Operations and intelligence functions must be consulted before this decision. However, the self-protection of combat aircraft and ships has priority over all controls. GUARDED, PROTECTED, and TABOO frequencies are defined as follows.

- **GUARDED.** GUARDED frequencies are adversary frequencies that are currently being exploited for combat information and intelligence. A GUARDED frequency is time-oriented in that the list changes as the adversary assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain against the loss of the technical information.
- **PROTECTED.** PROTECTED frequencies are those friendly frequencies used for a particular operation, identified, and protected to prevent them from being inadvertently jammed by friendly forces while active EW operations are directed against hostile forces. These frequencies are of such critical importance that jamming should be restricted unless absolutely necessary or until coordination with the using unit is made. They are generally time-oriented, may change with the tactical situation, and should be updated periodically.
- **TABOO.** TABOO frequencies are any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces. Normally these include international distress, CEASE BUZZER, safety, and controller frequencies. These are generally long-standing frequencies.

However, they may be time-oriented in that, as the combat or exercise situation changes, the restrictions may be removed to allow self protection by friendly forces. Specifically, during crisis or hostilities, short duration jamming may be authorized on TABOO frequencies for self protection to provide coverage from unknown threats, threats operating outside their known frequency ranges, or for other reasons.

f. **Disseminating the JRFL.** The JRFL is maintained and disseminated by the J-6.

g. **Updating the JRFL.** The JRFL is reviewed by all joint force staff sections and subordinate commands. The J-2 might need additions or deletions or qualified frequencies based on possible SIGINT and ES targets. The J-3 and IO cell monitor the JRFL with respect to changes in the operations, timing, dates, and TABOO frequencies. The J-6 ensures that PROTECTED frequencies are congruent with assigned frequencies. The J-6 also amends the JRFL based on input from J-2 and J-3. Supporting EW units check the JRFL because this list is the primary source of “no jam” frequencies.

3. JSIR Program

This program, coordinated and managed by the JSC, addresses those interference incidents that cannot be resolved at the unified, subordinate unified, JTF, and component levels. The JSIR program also satisfies the requirements of the Joint Staff and the stated needs of the CINCs for a joint-level agency to coordinate resolution of EMI incidents.

a. JSC has a 24-hour capability for receiving interference reports.

- Message address: JSC ANNAPOLIS MD//J3//

- Telephone: Defense Switched Network (DSN) (312) 281-9857, Commercial (410) 293-9857

- Sensitive compartmented information traffic is serviced directly through secure facsimile (FAX) and Intelink in the JSC sensitive compartmented information facility.

b. The following is the minimum information required for beginning a JSIR investigation.

- Information contained in component interference report.
- System affected by interference (nomenclature, J-12 number).
- Frequency of the victim receiver.
- The area or location where the interference incident occurred.
- Description of the interference.
- The time(s) and date(s) the interference occurred.
- A point of contact with DSN or commercial phone number and duty hours available to discuss the interference incident.

c. Upon receipt of a JSIR service request, the JSC JSIR team performs an analysis using JSC models and databases to determine the source and works with the appropriate field activity and frequency manager to resolve interference problems. Resources for geolocation and direction-finding support, as well as access to databases not resident at JSC, should be coordinated with appropriate agencies as necessary. The JSC JSIR team deploys to the location of the victim

organization, if necessary, in order to resolve interference problems. The organization requesting JSIR services is provided a report of the results of the JSIR analysis and appropriate information is incorporated into the JSIR database. This database supports trend analysis and future interference analysis. Space system interference reporting and resolution is similar to the terrestrial reporting and resolution process except that the interference report is sent directly to the Space Control Center (SCC) at United States Space Command, Cheyenne Mountain Air Station, Colorado (DSN 268-4405 or Commercial (719) 474-4405) from the space-system manager affected. The space system is considered to include both the space-based and earth segments. SCC forwards the incident report to the JSC for analysis.

4. Responsibilities

The responsibilities of the respective staff sections and commands in EW frequency deconfliction are noted below.

a. J-3 Responsibilities

- Determine and define critical friendly functions (TABOO and PROTECTED) to be protected from jamming and electronic deception based on the joint force concept of operations and in coordination with components.
- Approve the initial JRFL and subsequent changes.
- Provide guidance in OPLANs as to when jamming takes precedence over intelligence collection and vice versa.
- Resolve problems with the use of jamming and electronic deception in tactical operations when conflicts arise.

- Continually weigh the operational advantages of employing EW against the advantages of intelligence collection.
- Develop and promulgate specific ROE for jamming and electronic deception in support of combat operations. Coordinate ROE with Staff Judge Advocate.

b. J-2 Responsibilities

- In coordination with the national SIGINT authority, NSA, determine and define critical adversary functions and frequencies (GUARDED) and intelligence system processing and dissemination frequencies (PROTECTED) to be protected from friendly EA and provide them to the J-3 (through the IO cell) for approval.
- Assist in prioritizing the JRFL before J-3 approval.
- Develop and maintain map of nonmilitary entities operations on or near the area being jammed. Evaluate probable collateral effect on nonmilitary users.
- Nominate changes to the JRFL.
- Assist JSC in resolving reported disruption resulting from EMI.

c. J-6 Responsibilities

- Attempt to resolve all reported non-EA-related interference.
- Manage all frequency assignments for communications or non-communications equipment associated with the joint force.

- Maintain frequency databases of all joint force emitters (communications, non-communications equipment, radars, and jammers) to manage frequency assignments and assist the IO cell with resolving reports of interference through friendly EA.
- Compile, consolidate, coordinate, and disseminate the JRFL and provide the IO cell with the frequency assignments for those PROTECTED or TABOO unit nets that are designated for inclusion in the JRFL.
- Nominate changes to the JRFL based on the changing of assigned operational frequencies among friendly force units.
- Assist in minimizing adverse impact of friendly EA on critical networks by providing alternative communications.

d. EWO Responsibilities

- Attempt to resolve all reported EA-related interference.
- Coordinate and provide input to the JRFL.
- Recommend a joint force EW target list through the IO cell.
- Identify and resolve, if possible, conflicts that might occur between planned EA operations and the JRFL.
- Coordinate with J-6 and J-2 on reported interference to determine if friendly EA actions could be responsible.

e. Joint force subordinate commands and components should, where applicable, establish a unit staff element to perform the frequency deconfliction process. This staff element should be patterned after the IO cell and should be the focal point for frequency

deconfliction for the subordinate command and component forces it represents. The responsibilities of this frequency deconfliction staff element are as follows.

- Submits to the J-6, candidate nodes and nets (both friendly and adversary) with associated frequencies (if known), for inclusion in the JRFL using the format in Annex A, “Standardized JRFL Format.” Units should specifically designate only those functions critical to current operations for inclusion in the JRFL. Over-protection of nonessential assets complicates the EA support process and significantly lengthens the time required to evaluate mission impact resulting from spectrum protection. Normally, candidate nodes and nets should be submitted either through intelligence channels and consolidated by J-2 or through operations channels and consolidated by J-3.

- Identifies conflicts between JRFL and friendly EA operations and requests changes, as necessary, to resolve the conflicts.
- Reports unresolved spectrum disruption incidents as they occur in accordance with this publication and current interference reporting instructions.
- Keeps the IO cell apprised of EW planning and operational activities.

f. **JSC Responsibilities.** The JSC manages the DOD JSIR program as described in paragraph 3 above.

5. Frequency Deconfliction Analysis

Personnel analyzing frequency conflicts must consider frequency, location geometry, and time.

a. **Frequency.** The potential for interference exists whenever emitters (communications, non-communications equipment, radars, and jammers) operate at or close to the same frequency or range as unintended receivers. Interference can also occur through frequency harmonics throughout the EM spectrum with jamming operations. The JRFL limits the frequencies that require immediate review by the IO cell. Where possible, automated decision aids should be used to conduct this comparison.

b. **Location Geometry.** Because of the fluid nature of the battlefield (mobility), the locations of friendly emitters constantly change. The locations of friendly emitters should be analyzed by J-6 in order to predict possible interference. The results of the analyses depend highly on the accuracy, for example, of data and the analytical technique used.

c. **Time.** Time analysis attempts to protect critical communications network or non-communications equipment from friendly interference during friendly jamming missions. This subjective judgment is one that should be made by the J-3 or JTF commander, who must weigh the trade-off between critical jamming operations and protection of vital C2 resources.

will assist in developing and managing a constantly changing JRFL. To support a time and geographically oriented JRFL, automated systems must possess an engineering module that considers such factors as broadcast power, reception sensitivity, terrain, locations, distances, and time. The capability for direct computer data exchange between echelons for JRFL nominations and approval is recommended.

b. **Joint Spectrum Management System (JSMS) and SPECTRUM XXI.** JSMS and SPECTRUM XXI are computer-based systems that support the joint spectrum manager. JSMS and SPECTRUM XXI support operational planning as well as real-time management of the radio frequency spectrum, with emphasis on assigning compatible frequencies, deconflicting operations, and performing spectrum engineering tasks. During peacetime, JSMS and SPECTRUM XXI are used by a joint staff at its permanent headquarters to facilitate the complex task of managing the spectrum during the planning and execution phases of exercises, as well as performing routine spectrum management functions. In the combat environment, JSMS and SPECTRUM XXI are used by joint staffs to perform joint spectrum management. It is capable of implementing any variations between peacetime and wartime operations, such as operational area, frequency assignments, terrain data, equipment characteristics, and tactical constraints.

6. Automated Spectrum Management Tools

a. Commands are also encouraged to use automated spectrum management tools that

Intentionally Blank

ANNEX A TO APPENDIX B

STANDARDIZED JRFL FORMAT

The following JRFL format is an attempt to give the planner a standardized listing of information for developing a JRFL. This format is used by the JSMS. This sample JRFL is unclassified but, when actually accomplished, should show the proper classification of each paragraph.

1. CLASSIFICATION: One character (U=Unclassified, C=Confidential, S=Secret).
2. UNIT: Sixteen characters (net name as identified in communications-electronics operating instructions [CEOI]). Disregard for GUARDED nominations.
3. FREQUENCY: Twenty-four characters (K=kilohertz, M=megahertz, G=gigahertz, T=terahertz), identifies a frequency or band (e.g., M13.250-15.700).
4. STATUS: Four characters (T=TABOO /P=PROTECTED /G=GUARDED, and a slash followed by priority A-Z and 1-9 (e.g., T/A1).
5. PERIOD: Two characters (represents CEOI time period 01-10), if known.
6. START DATE: Eight characters (MM/DD/YY) indicates start date when protection is required, if known.
7. END DATE: Eight characters (MM/DD/YY) indicates end date when protection is no longer required, if known.
8. TRANSMITTER COORDINATES: Fifteen characters (latitude (dd[N r S] mmss)/longitude (ddd[E or W] mmss) provide the location to the transmitter or system, if known.
9. RECEIVER COORDINATES: Fifteen characters (latitude [dd(N or S)mmss] and longitude [ddd(E or W)mmss]) provides the location of the receiver or system to be protected, if known.
10. AGENCY SERIAL NUMBER: Ten characters (the agency serial number is a unique identifier for each frequency assignment), if known.
11. POWER: Nine characters (W=watts, K=kilowatts, M=megawatts, G=gigawatts) and a maximum of five decimal places, (e.g., W10.01234), if known.
12. EMISSION: Eleven characters (the emission designator contains the necessary bandwidth and the emission classification symbols [e.g., 3KOOJ3E]), if known.
13. EQUIPMENT NOMENCLATURE: Eighteen characters (e.g., AN/GRC-103), if known.
14. COMMENTS: Forty characters (provided for user remarks), optional entry.
15. CEOI NAME: Ten characters (a short title provided by the user to help identify the entry could use the actual title identified on the CEOI), optional entry.

Intentionally Blank

APPENDIX C

JOINT SPECTRUM CENTER SUPPORT TO JOINT ELECTRONIC WARFARE

1. General

The DOD JSC was activated on 28 September 1994. The JSC has assumed all the missions and responsibilities previously performed by the Electromagnetic Compatibility Center, as well as additional functions. The JSC is a field activity of the Defense Information Systems Agency.

2. Mission

The mission of the JSC is to ensure the Department of Defense's effective use of the EM spectrum in support of national security and military objectives. The JSC serves as the DOD center of excellence for EM spectrum management matters in support of the combatant commands, Military Departments, and Defense agencies in planning, acquisition, training, and operations. The JSC serves as the DOD focal point for supporting the spectrum supremacy aspects of IO. Since EW is a principal use of the spectrum within the IO effort, JSC support extends to the EW aspects of joint military operations.

3. The JSC Support to EW

a. The JSC provides data about friendly force C2 system locational and technical characteristics for use in planning electronic protect measures. Databases maintained by the JSC provide EW planners with information covering communications, radar, navigation aids, broadcast, identification, and EW systems operated by the Department of Defense, other United States Government departments and agencies, and private businesses or organizations. Information from these databases is available on a quick reaction basis in a variety of formats and media to

support EW planners and EM spectrum managers.

b. The JSC assists spectrum managers, EW planners, or the IO cell in the development of the JRFL. The JSC provides automated tools, JSMS and SPECTRUM XXI, to assist in the development and management of the JRFL and has designated CINC support teams that can be deployed to combatant commands, subordinate unified commands, JTFs, or their components when requested. These teams are trained to prepare JRFLs or provide training and assistance in how to prepare a JRFL. The teams can also serve as on-site advisors and assistants in EM spectrum management matters as required.

c. The JSC assists in the resolution of operational interference and jamming incidents through the auspices of the JSIR program. The objective of the JSIR program is to resolve problems at the lowest possible level in the chain of command. The JSC maintains rapid deployment teams that are able to quickly locate and identify interference sources. These teams recommend technical and operational fixes to resolve identified interference sources. The JSC also maintains a historical database of interference and jamming incident reports and solutions to assist in trend analysis and correction of recurring problems. Combatant commands, subordinate unified commands, JTFs, or their components should contact the JSC in order to request assistance in resolving suspected spectrum interference problems.

d. The JSC provides data about foreign command, control, and communications (C3) frequency and location data. Databases containing this data are developed primarily from open sources.

e. The JSC also provides unclassified C3 area studies about the C3 infrastructure of over 100 countries. These area studies are developed entirely from open source material. Information provided in these studies includes: physical and cultural characteristics (geography, climate, and population); overview of telecommunications systems; and EM frequencies registered for use within the geographic boundaries of each country. Data in these studies includes civilian, military, and radio and TV broadcast frequencies. Frequency data is provided in automated form to facilitate direct input into automated spectrum management tools such as the widely-used JSMS.

4. Mailing Address:

JSC/J3
2004 Turbot Landing
Annapolis, MD 21402-5064

5. Message Address:

JSC ANNAPOLIS MD//J3//

6. Telephone Numbers:

DSN: (312) 281-9815 (UNCLASSIFIED)
COMMERCIAL: (410) 293-9815
FAX: DSN (312) 281-3763 (UNCLASSIFIED)
FAX: DSN (312) 281-3684 (CLASSIFIED)
Duty Officer: DSN (312) 281-9857,
Commercial (410) 293-9857

APPENDIX D

ELECTRONIC WARFARE REPROGRAMMING

1. EW Reprogramming

a. **Purpose.** The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and TSS equipment maintained by field and fleet units. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems. The reprogramming of EW and TSS equipment is the responsibility of each Service through its respective EW reprogramming support programs.

b. **Types of Changes.** Several types of changes constitute EW reprogramming. These fall into three major categories: tactics, software, and hardware changes.

- **Tactics.** A tactics change includes changes in tactics, equipment settings, or EW systems mission-planning data. These changes are usually created and implemented at the unit level using organic equipment and personnel.
- **Software.** Software changes include actual changes to the software of programmable EW and TSS equipment. This type of change requires the support of a software support activity to alter programmed look-up tables, threat libraries, or signal-sorting routines. These changes are not normally created organically, although newer systems may be reprogrammed rapidly at the unit level using electronic transmission means.
- **Hardware.** Hardware changes and/or long-term system development is necessary when tactics or software changes cannot correct equipment deficiencies. These changes usually occur when the complex nature of a

change leads to a system modification. Hardware changes normally require depot-level support.

c. **EW Reprogramming Actions.** During crisis planning or actual hostilities, EW reprogramming provides operational commanders with a timely capability to correct EW and/or TSS equipment deficiencies, tailor equipment to meet unique theater or mission requirements, or to respond to changes in adversary threat systems.

- **Threat Changes.** Service EW reprogramming support programs are primarily designed to respond to adversary threat changes affecting the combat effectiveness of EW and TSS equipment. A threat change may be any change in the operation or EM signature of an adversary threat system.
- **Geographic Tailoring.** Geographic tailoring is the reprogramming of EW and TSS equipment for operations in a specific area or region of the world. Geographic tailoring usually reduces the number of threats in system memory, resulting in decreased processing time and a reduction in system display ambiguities.
- **Mission Tailoring.** Mission tailoring is the reprogramming of EW and TSS equipment for the mission of the host platform. Mission tailoring may be desirable to improve system response to the priority threat(s) to the host platform.

d. **General Reprogramming Process.** The reprogramming process for EW and TSS equipment can be divided into four phases. Although the last three phases of the reprogramming process are unique by Service,

each Service follows the general process described below.

- **Determine Threat.** The first phase of reprogramming is to develop and maintain an accurate description of the equipment's operational environment, specifically enemy threat systems and tactics. Since EW and TSS equipment is programmed to identify and respond to particular threat or target signature data, intelligence requirements must be identified to ensure that an accurate description of the EM environment is maintained at all times. Maintaining an accurate description of the environment requires fusion of known EM data with the collection, analysis, and validation of enemy "threat" signature changes. This first phase of the reprogramming process can be divided into the following three steps.

- **Collect Data.** Threat signature data collection (e.g., collection of threat system parametric information) is the responsibility of the combatant and component command collection managers. Signature data may be collected as a matter of routine intelligence collection against targeted systems, while other data collection may occur as the result of urgent intelligence production requests. Regardless of the means of collection, signature data is disseminated to appropriate intelligence production centers, and Service equipment support and flagging activities for analysis.

- **Identify Changes.** At Service support and flagging activities, collected signature data is analyzed for EW and TSS equipment compatibility. Incompatible data is "flagged" for further analysis and system impact assessment. At the intelligence production centers, collected data is processed and analyzed

to identify threat signature changes in the EM environment. Identified changes are further analyzed to ensure collector bias (i.e., collector contamination or manipulation of signature data attributed to the collector or its reporting architecture) was addressed during the analysis process.

- **Validate Changes.** The most important step of this initial phase of reprogramming is to validate threat signature changes. Therefore, once an identified signature change is correlated to a threat system and analyzed to ensure the reported parameters are correct and not a collector anomaly, it is further analyzed to "validate" it as an actual system capability change or identify it as a probable malfunction. Information on threat system engineering and tactical employment is critical to this validation process. Technical analysis and validation of threat changes is normally provided by one of three Service scientific and technical intelligence production centers or by the DIA. During times of crisis, the combatant command must ensure this phase of the reprogramming process provides for the expeditious identification, technical analysis, and dissemination of threat change validation messages to component commands and Service reprogramming centers.

- **Determine Response.** During this second phase of reprogramming, validated threat change information is used to assess its impact upon friendly EW and TSS equipment and a decision to initiate a reprogramming change is determined. If the equipment fails to provide appropriate indications and warning or countermeasures in response to a threat change, a decision must be made to change tactics, software, or hardware to correct the deficiency. To

support this decision making process, the Service reprogramming analysis or flagging activities normally generates a system impact message (SIM) to inform combatant and component command staffs of the operational impact of the threat change to EW and TSS equipment performance. The SIM often recommends appropriate responses for each identified threat change. The Service component employing the affected equipment is ultimately responsible for determining the appropriate response to validated threat changes.

- **Create Change.** The third phase of the reprogramming process is to develop tactics, software, or hardware changes to regain or improve equipment performance and combat effectiveness. A change in tactics (e.g., avoiding the threat) is usually the first option considered, because software and hardware changes take time. Often, a combination of changes (e.g., tactics and software changes) is prescribed to provide an immediate and long-term fix to equipment deficiencies. Regardless of the type of change created, reprogramming support activities will verify equipment combat effectiveness through modeling and simulation, bench tests, or test range employments simulating operational conditions. Following the verification of effectiveness, the reprogramming change and implementation instructions are made available to appropriate field and fleet units worldwide.
- **Implement the Change.** The final phase of the reprogramming process is to actually implement the change to ensure that unit combat effectiveness is regained or enhanced by the tactic, software, or hardware change. To accomplish this task, component commands ensure that

tactics changes are incorporated into mission pre-briefs, and software and hardware changes are electronically or mechanically installed in host platform EW and TSS equipment.

2. Joint Coordination of EW Reprogramming

a. **General.** Coordination of EW reprogramming is critical because threat signature changes and equipment reprogramming changes will affect the EM environment and all three subdivisions of joint EW operations. Combatant commands must ensure that joint coordination of EW reprogramming (JCEWR) policy and procedures are developed and exercised during all major training events and real-world operations.

b. **Policy.** The joint staff is responsible for JCEWR policy. Each Service is responsible for its individual EW reprogramming policies and procedures. The establishment and execution of JCEWR procedures is the responsibility of the combatant commands, component commands, and subordinate joint force commands in accordance with the following joint policy.

CJCSI 3210.04, “Joint EW Reprogramming Policy,” outlines the responsibilities of the Joint Staff, Military Services, combatant commands, Service components, NSA, and the DIA regarding the JCEWR process. The instruction also sets forth joint procedures, guidelines, and criteria governing joint intelligence support to EW reprogramming. This instruction describes the purpose of threat change validation and directs combatant commands to develop and exercise a timely threat change validation process to support the needs of component commands and Service reprogramming support activities during times of crisis.

Intentionally Blank

APPENDIX E

ELECTRONIC WARFARE MODELING

1. General

Digital models and simulations have become essential tools in the evaluation of EW and related systems. Simulations are critical because of the high cost of system development, field testing, and training exercises. Additionally, it is often impossible to replicate the multitude of variables and the interactions that occur in actual combat in a field test or training exercise.

2. Application

a. **Operational Test Support.** Test agencies use simulations to assist in planning and setting up field tests and in extrapolating, expanding, and verifying test results.

b. **Analysis Support.** Combat developers and other analysis activities use simulations to conduct cost and operational effectiveness studies, assist in defining requirements, perform force mix and tradeoff analyses, and develop tactics, doctrine, and procedures.

c. **Operational Support.** Operational commands use simulations to provide training from the individual to theater staff levels, perform as tactical decision aids, assist in developing and evaluating OPLANs, and conduct detailed mission planning.

d. **Weapon System Development.** Materiel developers use simulations to support engineering development and design, vulnerability and survivability analyses, and developmental testing.

e. **Intelligence Support.** Intelligence agencies use simulations to evaluate raw intelligence, develop threat projections, analyze threat design options, and evaluate threat tactics and employment options.

3. Modeling Agencies

There are numerous government agencies and contractors involved in EW modeling. The Joint Staff Director for Force Structure, Resource, and Assessment periodically publishes the “Catalog of Wargaming and Military Simulation Models.” This is the most comprehensive catalog of models available and identifies most agencies involved in EW modeling. Listed below are some of the joint and Service organizations involved with EW modeling and simulation.

a. **Joint.** Joint Command and Control Warfare Center, Joint Warfighting Analysis Center, Joint Spectrum Center, Warrior Preparation Center, and Joint Warfighting Center.

b. **Army.** Aviation and Missile Command, National Ground Intelligence Center, Air Defense Center and School, Intelligence Center and School, US Army Training and Doctrine Command Analysis Center, Electronic Proving Ground, Communications Electronics Command, Army Material Systems Analysis Agency, Test and Evaluation Command, Signal Center and School, and National Simulation Center.

c. **Navy.** Naval Command and Control and Ocean Surveillance Center, Naval Air Warfare Center, Naval Research Laboratory, Naval Strike Air Warfare Center, Naval Oceanographic Office, Center for Naval Analysis, Naval Space Command, and Naval Surface Warfare Center.

d. **Air Force.** Air Force Electronic Combat Office, Air Force Research Laboratory, National Air Intelligence Center, Air Force Information Warfare Center (AFIWC), Air Force Operational Test and Evaluation Center,

Air Force Studies and Analysis Agency, Aeronautical Systems Center, Survivability and Vulnerability Information Analysis Center, Air Armaments Center, Air and Space C2 Agency, C2 Battle Lab, and Air Force Wargaming Centers.

e. **Marine Corps.** Commandant's Warfighting Lab, Wargaming and Combat Simulated Division of Marine Corps Combat Development Command, and MAGTF Staff Training Program, Modeling and Simulation Branch.

4. Fidelity Requirements

Fidelity is the degree of accuracy and detail to which the environment, physical entities, and their interactions are represented. Fidelity requirements vary widely depending on the particular application. Considerations in determining the proper fidelity should be based on scope (e.g., individual versus corps staff), consequences of inaccurate results (e.g., air strike against sophisticated air defense), time available, computer resources available, accuracy of available data, and allowable tolerance of results. Regardless of the fidelity required, a consistent analytic approach should be used. As an example, table look-up values for a low resolution model could be obtained from a high resolution model. An audit trail should be available in an analyst manual or other documentation to determine simplifying assumptions, limitations, and aggregation techniques. In general, the model setup time, run time, and user expertise required increase as model scope, fidelity, and flexibility increase.

5. Model Design

a. **User Interface, Preprocessors, and Postprocessors.** These requirements will vary widely depending on the particular application. For example, a radar design engineer will need much more flexibility and detail for input data than a targeting analyst

would need in a tactical decision aid. Other than purpose, setup, and analysis, time requirements and user expertise are key considerations in designing preprocessors and postprocessors and the user interface. In general, maximum use should be made of standard graphic user interfaces.

b. **Electronic Warfare Functions.** For mission planning or force level analysis, all EW functions need to be represented to some extent. For other applications, the specific purpose will drive what functions should be represented. EW model functions include such areas as propagation, radio line of sight, self-protect jamming, standoff jamming (communications and non-communications), ES vulnerability and effectiveness, expendables effectiveness (chaff and flares), decoy effectiveness (active and passive), SEAD, acquisition and tracking (radar, electro-optical and infrared), clutter effects, satellite coverage and link analysis, missile flyout (effects of countermeasures), effects of evasive maneuvers, C3 processes, EP, and effects of lethal attack on critical C3 nodes.

c. **Software Architecture.** The design of an EW model or system of models should be modular and object oriented. Existing standards and commonly used commercial software packages should be used where appropriate. Standards include those from the Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute, Federal Information Processing Standards, Military Standard 2167A, Open Software Foundation, and National Security Agency and Central Security Service. 2167A standards should be tailored to meet the user requirements for documentation. Standards are particularly important with regard to interfaces. The primary objective of standardization is to make the simulation as machine independent as possible. To this end, the operating system environment should conform to IEEE Portable Operating System Interface for

Computer Environments standards. Additionally, communications protocols and interfaces should conform to the Government Open Systems Interconnection Profile, which is the DOD implementation of international Open Systems Interconnect standards.

6. Verification and Validation

a. **Verification.** Model verification is related to the logic and mathematical accuracy of a model. Verification is accomplished through such processes as design reviews, structured walk-throughs, and numerous test runs of the model. Test runs are conducted to debug the model as well as determine the sensitivity of output to the full range on input variables. Included in verification is a review of input data for consistency, accuracy, and source. Ultimately, verification determines if the model functions as designed and advertised. Verification is rather straightforward but time consuming.

b. Validation

- Model validation relates to the correlation of the model with reality. In general as the scope of a simulation increases, validation becomes more difficult. At the engineering level for a limited scope problem, it is often possible to design a laboratory experiment or field test to replicate reality. At the force level, it is not possible to replicate all the variables on the battlefield and their interaction. It may be possible to validate individual functional modules by comparison with test data or previously validated engineering-level or high to medium resolution models. No model totally represents reality, and this disparity increases as the model scope increases. At the force level, models can provide relative answers, insights, and trends so that alternatives may be rank ordered. Any model user should always keep

model limitations and assumptions in mind and use the model in conjunction with off-line methods to compensate for these shortfalls.

- Although the above methods may be used for the validation of individual modules in a force level model, three techniques are used for validating the bottom line output of force-on-force simulations: benchmarking with an accepted simulation, comparing with historical data, and using military judgment. As technological advances are rapidly being incorporated in modern forces, historical data is becoming less useful for predicting outcomes in a future mid- to high-intensity conflict. Military judgment is still a viable method but is biased by the unique experience of the person or persons making the judgment. Benchmarking with an accepted simulation provides the most straightforward and least biased method of validation. The primary problem here is caused by differing data structures between the models. However, by careful review and manipulation of input data, this problem can be minimized to preclude “comparing apples to oranges.”

7. Databases

Numerous databases are available to support EW modeling. Data include doctrinal, order of battle, parametric, signature, antenna pattern, C3 networks, and topographic. One of the most comprehensive database catalogs available is the directory of DOD-Sponsored Research and Development databases produced by the Defense Technical Information Center. Some sources of data for EW modeling include the following.

- a. **Doctrinal or Scenario Order of Battle and C3 Networks.** DIA, Combined Arms Center, National Ground Intelligence Center

(NGIC), National Air Intelligence Center, AFIWC, Naval Weapons Center, and Air Force Air Warfare Center.

b. **Parametric Signature Antenna Pattern.** NSA, NGIC, Missile and Space Intelligence Center, JSC, AFIWC, and DIA.

c. **Topographic.** NIMA, US Geological Survey, Army Engineer Topographic Laboratories, CIA, and Waterways Experiment Station.

APPENDIX F

SERVICE PERSPECTIVES OF ELECTRONIC WARFARE

1. Army

The focus of Army EW operations is based on the need to synchronize lethal and nonlethal attacks against adversary C3 targets. Army EW disrupts, delays, diverts, and denies the adversary while protecting friendly use of communications and non-communications systems. The perspective of Army forces is directly associated with the combined arms structure of adversary forces and the manner in which both friendly and adversary combatants conduct combat operations. The high mobility of opposing combat forces and the speed, range, precision accuracy, and lethality of their weapons systems place stringent demands on the C2 systems of both friendly and adversary ground force commanders. Synchronization is achieved by integrating EW into both the IO plan and fire support operations in support of the ground scheme of maneuver, using centralized control and decentralized execution functions performed by parallel C3 systems and procedures at all echelons. Organic EW resources available to support Army operations are limited. Mission requirements usually exceed operational capability. Cross-Service EW support, synchronized with Army combat operations, is essential to the success of joint military operations. Joint planning and continuous, effective coordination are critical to synchronizing joint EW capabilities and generating joint combat power at the critical time and place in battle. The Army provides and requires cross-Service EW support when and where needed to achieve the combat objectives and operational goals of the JFC.

2. Marine Corps

The Marine Corps employs EW within the concept of maneuver warfare with the intent

to disrupt the adversary's ability to command and control forces, thereby influencing the enemy's decision cycle. This ability enhances friendly capabilities while shattering the moral, mental, and physical cohesion of the adversary, rendering the adversary incapable of effectively resisting. Marine EW units, found within both the command and aviation combat elements of a MAGTF, are task-organized to meet the needs of the MAGTF commander, subordinate commanders, and ultimately the operational goals of the JFC. EW units are integrated into the commander's concept of operations and scheme of maneuver in order to enhance the MAGTF's inherent combined arms capabilities. Through this integration of aviation and ground EW capabilities, the MAGTF is able to exploit both the long- and the short-term effects of EW, conducting active operations of EA, ES, and EP in order to support the operational requirements of the MAGTF commander as well as those of the JFC with provision of cross-Service support in the joint arena.

3. Navy

Naval task forces use all aspects of space and EW in performing their naval warfare tasks. Emphasis is given to surveillance, the neutralization or destruction of adversary targets, and the enhancement of friendly force battle management through the integrated employment and exploitation of the EM spectrum and the medium of space. Naval battle groups employ a variety of organic shipboard EW systems, primarily for self protection. Naval aviation forces are the primary means by which naval forces take the EW fight to the adversary at extended ranges. Carrier and land-based EA-6B Prowlers use a variety of onboard systems to conduct EA (including both standoff and close-in jamming), ES, and EP in support of SEAD

and IO tasking. Naval task force use of the EM spectrum and space encompasses measures that are employed to:

- Coordinate, correlate, fuse, and employ aggregate communication, surveillance, reconnaissance, data correlation, classification, targeting, and electromagnetic attack capabilities;
- Deny, deceive, disrupt, destroy, or exploit the adversary's capability to communicate, monitor, reconnoiter, classify, target, and attack;
- Facilitate anti-ship missile defense; and
- Direct and control employment of friendly forces.

4. Air Force

The COMAFFOR conducts a variety of EW operations, including EA, EP, and ES. In addition, EW supports SEAD and IO. The object of these operations is to increase aircraft survivability, enhance the effectiveness of military operations, and increase the probability of mission success. Air Force EW system development and

employment focus on this task. The Air Force uses an integrated mix of disruptive and destructive EW systems to defeat hostile integrated air defenses. Disruptive EW systems, (e.g., self-protection jamming) provide an immediate but temporary solution. The EC-130H Compass Call is the Air Force's primary nonlethal SEAD asset. It performs C3 countermeasures throughout the C2 spectrum, supporting air, land, sea, and special operations across the range of military operations. Destructive systems provide a more permanent solution, but may take longer to fully achieve the desired results. The integrated use of destructive and disruptive systems offsets their individual disadvantages and results in a synergistic effect. Successful EW operations emphasize risk reduction while still maintaining mission effectiveness. The military significance of EW is directly related to the increase in mission effectiveness and to the reduction of risk associated with attaining air superiority. Aggressive employment of EW can have a profound impact on the JFC's IO. The Air Force employs a variety of ground-, air-, and space-based assets to accomplish these tasks.

APPENDIX G

REFERENCES

The development of JP 3-51 is based upon the following primary references.

1. DOD Directive 3222.3, “DOD Electromagnetic Compatibility Program.”
2. DOD Directive 3222.4, “Electronic Warfare (EW) and Command and Control Warfare Countermeasures.”
3. CJCSI 3121.01, “Standing Rules of Engagement for US Forces.”
4. CJCSI 3150.25, “Joint After-Action Reporting System.”
5. CJCSI 3210.01, “Joint Information Operations Policy.”
6. CJCSI 3210.03, “Joint Electronic Warfare Policy.”
7. CJCSI 3210.04, “Joint EW Reprogramming Policy.”
8. CJCSI 3220.01, “Electromagnetic Spectrum Use in Joint Military Operations.”
9. CJCSI 3221.01, “Near Real-Time Analysis of Electromagnetic Interference and Jamming of US Space Systems.”
10. CJCSI 6510.01, “Defensive Information Warfare Implementation.”
11. CJCSM 3122.03, “Joint Operation Planning and Execution System Vol II: (Planning Formats and Guidance).”
12. CJCSM 3212.02, “Performing Electronic Attack in the United States and Canada.”
13. CJCSM 3220.01, “Joint Operations in the Electromagnetic Battlespace.”
14. CJCSM 3500.03, “Joint Training Manual for the Armed Forces of the United States.”
15. CJCSM 3500.04B, “Universal Joint Task List.”
16. JP 1-02, “DOD Dictionary of Military and Associated Terms.”
17. JP 1-04, “Joint Tactics, Techniques, and Procedures for Legal Support to Military Operations.”
18. JP 2-0, “Doctrine for Intelligence Support to Joint Operations.”
19. JP 2-01, “Joint Intelligence Support to Military Operations.”

20. JP 2-02, “National Intelligence Support to Joint Operations.”
21. JP 3-01.4, “Joint Tactics, Techniques, and Procedures for Joint Suppression of Enemy Air Defenses (J-SEAD).”
22. JP 3-05, “Doctrine for Joint Special Operations.”
23. JP 3-09, “Doctrine for Joint Fire Support.”
24. JP 3-13, “Joint Doctrine for Information Operations.”
25. JP 3-53, “Doctrine for Joint Psychological Operations.”
26. JP 3-54, “Joint Doctrine for Operations Security.”
27. JP 3-57, “Doctrine for Joint Civil Affairs.”
28. JP 3-58, “Joint Doctrine for Military Deception.”
29. JP 3-61, “Doctrine for Public Affairs in Joint Operations.”
30. Air Land Sea Application Center publication “Multiservice Tactics, Techniques, and Procedures for EA-6B Employment in the Joint Environment.” (Referenced by individual Services as FM 90-39, MCRP 3-22A, NWP 3-01.4, and AFTTP(I) 3-2.4.)
31. MC 64/7, NATO “Electronic Warfare Policy.”
32. AJP-01(A), “Allied Joint Operations Doctrine.”
33. ATP-8A, “Doctrine for Amphibious Operations.”
34. ATP-44, “Electronic Warfare in Air Operations.”
35. ATP-51, “Electronic Warfare in the Land Battle.”
36. QSTAG 593, “Doctrine on Mutual Support Between EW Units.”
37. QSTAG 1022, “Electronic Warfare in the Land Battle.”

APPENDIX H

ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command, Joint Warfighting Center Code JW100, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

3. Supersession

This publication supersedes JP 3-51, 30 June 1991, “Electronic Warfare in Joint Military Operations.”

4. Change Recommendations

- a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J39/STOD//
INFO: JOINT STAFF WASHINGTON DC//J7-JDD//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, DC 20318-7000.

- b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

- c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

5. Distribution

- a. Additional copies of this publication can be obtained through Service publication centers.
- b. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PSS, Room 1A674, Pentagon, Washington, DC 20301-7400.
- c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

Army:	US Army AG Publication Center SL 1655 Woodson Road Attn: Joint Publications St. Louis, MO 63114-6181
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Commander (Attn: Publications) 814 Radford Blvd, Suite 20321 Albany, GA 31704-0321
Coast Guard:	Commandant (G-OPD), US Coast Guard 2100 2nd Street, SW Washington, DC 20593-0001 Commander USJFCOM JWFC Code JW2102 Doctrine Division (Publication Distribution) 116 Lake View Parkway Suffolk, VA 23435-2697

- d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

GLOSSARY

PART I — ABBREVIATIONS AND ACRONYMS

A-3	Operations Directorate (COMAFFOR)
A-5	Plans Directorate (COMAFFOR)
AAR	after-action report
ABCA	American, British, Canadian, Australian Armies Standardization Program
AFIWC	Air Force Information Warfare Center
AGCCS	Army Global Command and Control System
AJP	Allied Joint Pub
ASCC	Air Standardization Coordinating Committee
ATO	air tasking order
ATP	Allied Tactical Pub
C2	command and control
C3	command, control, and communications
CAG	carrier air group
CAP	crisis action planning
CCIR	commander's critical information requirements
CIA	Central Intelligence Agency
CINC	commander of a combatant command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
COA	course of action
COMAFFOR	Commander, Air Force Forces
COMSEC	communications security
CVWC	carrier battle group air wing commander
CWC	composite warfare commander
DE	directed energy
DEW	directed-energy warfare
DIA	Defense Intelligence Agency
DOD	Department of Defense
DSN	Defense Switched Network
DSO	defensive systems officer
E3	electromagnetic environmental effects
EA	electronic attack
ECO	electronic combat officer
EEFI	essential elements of friendly information
ELINT	electronic intelligence
EM	electromagnetic
EMC	electromagnetic compatibility

EMCON	emission control
EME	electromagnetic environment
EMI	electromagnetic interference
EOB	electronic order of battle
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
EWCC	electronic warfare coordination center
EWO	electronic warfare officer
FAX	facsimile
FPC	final planning conference
FSE	fire support element
G-3	Army or Marine Corps component operations staff officer
G-6	Army or Marine Corps component command, control, communications, and computer systems staff officer
GCCS	Global Command and Control System
HERO	hazards of electromagnetic radiation to ordnance
IEEE	Institute of Electrical and Electronics Engineers
IO	information operations
IPC	initial planning conference
IWC	information warfare commander
J-2	Intelligence Directorate of a joint staff
J-3	Operations Directorate of a joint staff
J-5	Plans Directorate of a joint staff
J-6	Command, Control, Communications, and Computer Systems Directorate of a joint staff
JAC	Joint Analysis Center
JCA	jamming control authority
JCEWR	joint coordination of electronic warfare reprogramming
JECG	joint exercise control group
JFACC	joint force air component commander
JFC	joint force commander
JFMO	joint frequency management office
JFSOCC	joint force special operations component command
JIC	Joint Intelligence Center
JISE	joint intelligence support element
JOC	Joint Operations Center
JOPES	Joint Operation Planning and Execution System
JP	joint publication
JRFL	joint restricted frequency list
JSC	Joint Spectrum Center
JSIR	Joint Spectrum Interference Resolution
JSMS	Joint Spectrum Management System

JTF	joint task force
LOAC	law of armed conflict
MAGTF	Marine air-ground task force
MASINT	measurement and signature intelligence
MC	Military Committee (NATO)
MNFC	multinational force commander
MNF	Multinational Force
MPC	mid-planning conference
MSEL	master scenario events list
NATO	North Atlantic Treaty Organization
NGIC	National Ground Intelligence Center
NIMA	National Imagery and Mapping Agency
NMJIC	National Military Joint Intelligence Center
NSA	National Security Agency
OIC	officer in charge
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PSYOP	psychological operations
QSTAG	Quadripartite Standardization Agreement (NATO)
RADBN	radio battalion
ROE	rules of engagement
S-3	battalion or brigade operations staff officer (Army; Marine Corps battalion or regiment)
SCC	Space Control Center
SEAD	suppression of enemy air defenses
SIGINT	signals intelligence
SIM	system impact message
SO	special operations
SOP	standard operating procedure
STARTEX	start of the exercise
TSS	target sensing system
USCG	United States Coast Guard
VMAQ	Marine tactical electronic warfare squadron
WARM	wartime reserve modes
WP	Working Party (NATO)

PART II — TERMS AND DEFINITIONS

CEASE BUZZER. An unclassified term to terminate electronic attack activities, including the use of electronic warfare expendables. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

civil affairs. The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Also called CA. (JP 1-02)

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the

accomplishment of the mission. Also called C2. (JP 1-02)

communications intelligence. Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (JP 1-02)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. a. — cryptosecurity. The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. — transmission security. The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. — emission security. The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. — physical security. The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP 1-02)

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA. Also called CNA. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

computer network defense. Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Also called CND. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

directed energy. An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. Also called DE. (JP 1-02)

directed-energy device. A system using directed energy primarily for a purpose other than as a weapon. Directed-energy devices may produce effects that could allow the device to be used as a weapon against certain threats, for example, laser rangefinders and designators used against sensors that are sensitive to light. (JP 1-02)

directed-energy warfare. Military action involving the use of directed-energy weapons, devices, and countermeasures to

either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. (JP 1-02)

directed-energy weapon. A system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel. (JP 1-02)

electromagnetic compatibility. The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness. Also called EMC. (JP 1-02)

electromagnetic deception. The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are: a. manipulative electromagnetic deception. Actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces. b. simulative electromagnetic deception. Actions to

simulate friendly, notional, or actual capabilities to mislead hostile forces. c. imitative electromagnetic deception. The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. (JP 1-02)

electromagnetic environmental effects. The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility/electromagnetic interference; electromagnetic vulnerability; electromagnetic pulse; electronic protection, hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and p-static. Also call E3. (JP 1-02)

electromagnetic interference. Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like. Also called EMI. (JP 1-02)

electromagnetic intrusion. The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operations or of causing confusion. (JP 1-02)

electromagnetic jamming. The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. (JP 1-02)

electromagnetic pulse. The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. Also called EMP. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

electromagnetic spectrum. The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02)

electronic intelligence. Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (JP 1-02)

electronic masking. The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/signals intelligence, without significantly degrading the operation of friendly systems. (JP 1-02)

electronic probing. Intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices or systems. (JP 1-02)

electronic reconnaissance. The detection, location, identification, and evaluation of foreign electromagnetic radiations. (Upon approval of this revision, this term and its definition will modify the existing term and

its definition and will be included in JP 1-02.)

electronics security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar. (JP 1-02)

electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize

sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

electronic warfare frequency deconfliction.

Actions taken to integrate those frequencies used by electronic warfare systems into the overall frequency deconfliction process. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

electronic warfare reprogramming. The deliberate alteration or modification of electronic warfare (EW) or target sensing systems (TSS), or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. These changes may be the result of deliberate actions on the part of friendly, adversary or third parties; or may be brought about by electromagnetic interference or other inadvertent phenomena. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and TSS equipment. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

emission control. The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. minimize mutual interference among friendly systems; and/or c. execute a military deception plan. Also called EMCON. (JP 1-02)

frequency deconfliction. A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management. (JP 1-02)

guarded frequencies. Enemy frequencies that are currently being exploited for combat information and intelligence. A guarded frequency is time-oriented in that the guarded frequency list changes as the enemy assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain against the loss of the technical information. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

imitative communications deception. That division of deception involving the introduction of false or misleading but plausible communications into target systems that mimics or imitates the targeted communications. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (JP 1-02)

joint restricted frequency list. A time and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. It should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. Also called JRFL. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

joint suppression of enemy air defenses. A broad term that includes all suppression of enemy air defenses activities provided by one component of a joint force in support of another. Also called J-SEAD. (JP 1-02)

meaconing. A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. (JP 1-02)

measurement and signature intelligence. Intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted. Also called MASINT. (JP 1-02)

military deception. Actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are: a. strategic military

deception—Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator’s strategic military objectives, policies, and operations. b. operational military deception—Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator’s objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations. c. tactical military deception—Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator’s objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. d. Service military deception—Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems. e. military deception in support of operations security (OPSEC)—Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities. (JP 1-02)

Modernized Integrated Database. The national level repository for the general military intelligence available to the entire Department of Defense Intelligence Information System community and, through Global Command and Control System integrated imagery and intelligence, to tactical units. This data is maintained and updated by the Defense

Intelligence Agency. Commands and Services are delegated responsibility to maintain their portion of the database. Also called MIDB. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

nondestructive electronic warfare. Those electronic warfare actions, not including employment of wartime reserve modes, that deny, disrupt, or deceive rather than damage or destroy. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- a. Identify those actions that can be observed by adversary intelligence systems.
- b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 1-02)

precipitation static. Charged precipitation particles that strike antennas and gradually charge the antenna, which ultimately discharges across the insulator, causing a burst of static. Also called P-STATIC. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

protected frequencies. Those friendly frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electronic warfare operations are directed against hostile forces. These frequencies are of such critical importance that jamming

should be restricted unless absolutely necessary or until coordination with the using unit is made. They are generally time-oriented, may change with the tactical situation, and must be updated periodically. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (JP 1-02)

public affairs. Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA. (JP 1-02)

signal security. A generic term that includes both communications security and electronics security. (JP 1-02)

signals intelligence. 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. (JP 1-02)

spectrum management. Planning, coordinating, and managing joint use

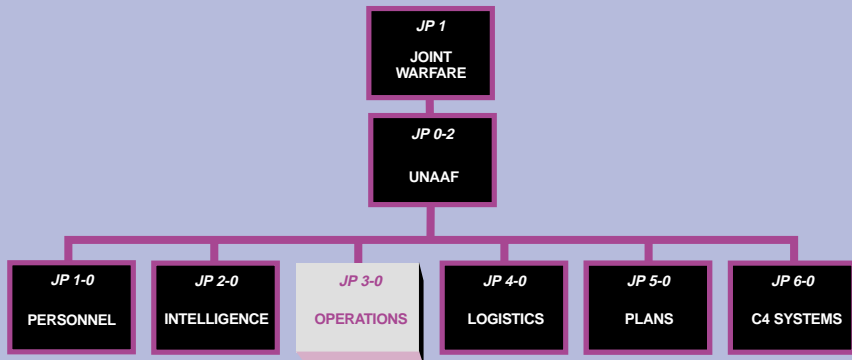
of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. (JP 1-02)

suppression of enemy air defenses. That activity which neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means. Also called SEAD. (JP 1-02)

TABOO frequencies. Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces. Normally, these frequencies include international distress, CEASE BUZZER, safety, and controller frequencies. These frequencies are generally long standing. However, they may be time-oriented in that, as the combat or exercise situation changes, the restrictions may be removed. (Upon approval of this revision, this term and its definition will be included in the next edition of JP 1-02.)

wartime reserve modes. Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. Wartime reserve modes are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use. Also called WARM. (JP 1-02)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-51** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

